universität wien

DISSERTATION

Titel der Dissertation

„Transnational Organized Crime in the Context of Internet“

Verfasserin

Xiangxia LI

angestrebter akademischer Grad

Doktorin der Rechtswissenschaften (Dr.iur.)

Wien, 2015

Studienkennzahl lt. Studienblatt:	A 783 101
Dissertationsgebiet lt. Studienblatt:	Rechtswissenschaften
Betreuerin:	Univ.-Prof. Dr. Susanne Reindl-Krauskopf

Contents

Preface

Transnational organized crime[1] is one of the most serious threats faced by human beings in the new 21 century, but as the proliferation of internet information technology spreads, new challenges are posed to researchers and law enforcement agencies in the world. Economic globalization and information technology are double swords, which bring much convenience to human life, while at the same they also provide chances for transnational organized criminal groups. In this context, this dissertation mainly analyzes the following topics: evolution of organized crime, the concepts of transnational organized crime and cyber transnational organized crime, features and new trends of organized crime in the era of the internet, sorting out and investigating criminal legislation and the adjustment of criminal policy combating cyber transnational organized crime, Dilemmas of the Joint Crime Theory and corresponding Resolutions under Cyber Transnational Organized Crime (CTOC). This dissertation includes 250 cases concerning transnational organized crime which combine with factors of internet information technology, and by means of analyzing new features of these cases, the changes and tendencies of organized crime will be discussed in the era of the internet. Under the circumstance of internet information technology, two significant tendencies of transnational organized crime should be paid noted, namely, there are two main threads running through the whole thesis. One is the internationalization of traditional organized crime with the assistance of internet information technology, for example, traditional trafficking in persons and drugs. Another is that a new trend in which, almost all types of crime are developing a transnational character and are organized by means of internet information technology, has been identified. This thesis focuses on analyzing the present situation, new characteristics and developing trends of transnational organized crime, on grasping new challenges of criminal theories, domestic law and international law, and finally on proposing effective measures against transnational

[1] Traditional organized crime in this dissertation indicates such organized crimes as might have been carried out prior to the emergence of the internet, i.e., crimes which can be committed without using the internet.

organized crime in the context of internet. Obviously, at present the United Nations Convention Against Transnational Organized Crime (UNTOC) is not enough to cope with these new changes of transnational organized crime in the era of the internet, scholars and all kinds of law enforcement agencies need to do more, and there is long way to go.....

Abbreviations

CISC	Criminal Intelligence Service Canada
CID	Criminal Investigation Division
CTOC	Cyber Transnational Organized Crime
CTOCG	Cyber Transnational Organized Criminal Group
CTOCGs	Cyber Transnational Organized Criminal Groups
COC	Cyber Organized Crime
DCPCU	the Dedicated Cheque and Plastic Crime Unit
ELN	National Liberation Army
EPL/D	People's Liberation Army
etc	et cetera
FARC	Revolutionary Armed Force of Columbia
FBI	Federal Bureau of Investigation
HTCU	Vietnamese High-Tech Crime Unit
ICE	Italian Criminal Enterprises
ICTs	Information Communication Technologies
i.e.	id est
Interpol	International Criminal Police Organization
LCN	La Cosa Nostra
MPSVN	Ministry of Public Security of Vietnam

NCA	National Crime Authority of Australia
NCIS	the National Criminal Intelligence Service of the United Kingdom
NSW	the New South Wales
OC	Organized Crime
OCG	Organized Criminal Group
OCGs	Organized Criminal Groups
PCeU	Police Central e-crime Unit
PRC	the People's Republic of China
RICO	the Racketeer Influenced and Corrupt Organizations Act
SOCA	Serious Organised Crime Agency
TOC	Transnational Organized Crime
TOCG	Transnational Organized Criminal Group
TOCGs	Transnational Organized Criminal Groups
UNODC	the United Nations Office on Drugs and Crime
UNTOC	the United Nations Convention against Transnational Organized Crime

Chapter 1 Evolution of Organized Crime since the 1950s and its concept

Introduction

The phenomenon of crime is a long-rooted chronic disease of civilized society. Generally speaking, the harmfulness and gravity of crimes, which are committed by a solitary perpetrator, Organized Criminal Groups (OCGs), transnational organized criminal groups and Cyber Transnational Organized Criminal Groups (CTOCGs), are increasing. During the evolution of Organized Crime (OC), there are three phases: according to Peter Lupsha. He referred to "degrees" of organized crime two years ago, and these three phases include: a first "predatory" one, marked by the use of violence to gain control of a given territory; a second "corrupting" one, during which period the organized criminal group established relations with the legitimate state authorities; eventually, a third "symbiotic" stage, which means the Organized Criminal Groups (OCGs) merged with state authorities, this being an indispensable move to gain social legitimacy. [2] This argument took a "microcosmic" standpoint to analyze the development of organized crime.[3] In this chapter the evolution of OC is introduced on the basis of a "macroscopic" perspective.[4] So in the following text of this chapter, the situation of Transnational Organized Crime (TOC) in the context of the internet in Europe, Asia, North America, South America and Australia will be discussed respectively. The second section introduces certain types of definition of OC. Finally,

[2] Gianluca Fulvetti, The Mafia and the " Problem of the Mafia": Organized Crime in Italy, 1820-1970, In Cyrille Fijnaut and Letizia Paoli (ed.) (2004), Organized Crime in Europe: *Concepts Patterns and Control Policies in the European Union and Beyond*, Springer, p.47.

[3] The microcosmic standpoint refers to analyzing certain organized criminal groups to introduce the development of organized crime rather than analyzing the development of organized crime by regarding it as a general phenomenon in the whole of society.

[4] Macroscopical perspective is the opposite of microcosmic standpoint, which means that considering the organized crime as a general phenomenon in some certain regions when introducing the evolution of organized crime instead of analyzing the particular cases concerning organized crime.

on the basis of these definitions, a concept of CTOC, which is proposed by this dissertation, will be concluded in this part.

Section 1 Evolution of Organized Crime since the 1950s

It is generally acknowledged that TOC evolves from OC, so it is necessary to give a brief introduction concerning the historical development of OC since the 1950s of the last century for the following contents of this thesis. The modern history of organized crime reveals its characteristics, which further provides the basis for concluding the concept of OC in section 2.

1. Evolution of European Organized Crime

Generally speaking, since the earlier completion of the industrial revolution provided fertilizer and better conditions for the development of European organized crime, the formation and development of organized crime in European countries, like England Russia and Italy were much earlier than in the countries in other regions.[5]

1.1 Italy

Organized crimes in Italy are usually associated with those criminal activities of the "Mafia", since 1860s this term has been used to describe the widespread manifestations

[5] Lu Jianping eds. *Comparative Study of Organized Crime*, Law Press • China, 2004, P.4.

of OC in the southern regions of the country.[6] According to their geographic origin, by far the most recognized grouping, the Sicilian mafia, the Calabrian 'Ndrangheta and the Campanian camorra have intertwined their criminal history with the wider one of the Italian social, political and economic development.[7] All the three organizations can be called "mafias" due to two reasons. On the one hand, the natures of them are the same. On the other hand, the Italian government authorities usually do so, in the bi-annual reports presented by the Direzione Investigativa Antimafia and the anti-mafia central investigating office to the Parliament in which Sicilian mafia, Calabrian 'Ndrangheta and campanian camorra are all included in the category "Organized Crime of Mafia Type".[8]

Even though the three above-mentioned criminal associations have their own traditions, they have common natures that are reflected by a great number of points in common and similarities among them. Obviously, the types of their criminal activities are good instances to illustrate these similarities, since the Sicilian mafia, Calabrian 'Ndrangheta and campanian camorra carried out the following types of crimes, in the aspect of the traditional illicit field, such as fraud, prostitution, kidnap, extortion and traffic in drugs. In the 60-70s of the last century, all of these criminal associations made an expansion of illicit markets in Sicily. As a result, the "industry of violence" found new sources of economic gain.[9] This expansion is reflected by the illicit area of new drugs and arms markets. Apart from that, this expansion is also illustrated by the geographical location of their criminal activities, not only can their trace be found in the other regions of Italy, but also their influence began to penetrate into the other countries of Europe, North and

[6] Gianluca Fulvetti, The Maifa and the " Problem of the Mafia": Organized Crime in Italy, 1820-1970, In Cyrille Fijnaut and Letizia Paoli (ed.) (2004), Organized Crime in Europe: *Concepts Patterns and Control Policies in the European Union and Beyond*, Springer, p.48.

[7] Sean Grennan and Marjie T. Britz, *Organized Crime: a Worldwide Perspective*, Pearson Education, Inc.,Upper Saddle River, New Jersey, 2006, p.30-33.

[8] These bi-annual reports were presented by the Direzione Investigativa Anti-mafia and the anti-mafia central investigating office to the Parliament, cited in Gianluca Fulvetti, The Mafia and the "Problem of the Mafia": Organized Crime in Italy, 1820-1970, In Cyrille Fijnaut and Letizia Paoli (ed.) (2004), *Organized Crime in Europe: Concepts Patterns and Control Policies in the European Union and Beyond*, Springer, p.48.

[9] Ibid, p.68.

South American and Asian. Since the end of the 1970s mafia "violent entrepreneurs" began to exert pressure on the political system, and this change resulted in the murder of numerous politicians and state officials and in a final clash between the state and the mafia in the early 1990s. Thus, the last 20 years of the last century undoubtedly reveal the best known period in the history of Italian organized crime and witness very significant events, ranging from the bomb explosions staged by the Sicilian Cosa Nostra in 1992 and 1993 to the trial of Giulio Andreotti.[10] In the past dozen years, on the one hand, in order to carry out criminal activities on a larger scale and diminish the detriment from those countries which have all-inclusive legal systems and substantive experience concerning anti-organized crime, Italian mafia criminal associations have promptly and smartly taken the chances of internationalization of commercial and financial markets, the disappearance of all kinds tariff barriers, the improvement of science and technology, and the opportunities provided by situation of new global geopolitics, by which they positively seek the international market and room to expand the extent of their illegal activities and their influence to other countries and regions. On the other hand, Italian mafia organizations also bribe state officials of their country and other countries who usually hold significant public powers, these crimes are usually connected with money laundering.

In the above short introduction, a brief development of the Italian mafia has been presented. The basic internal structure of the Sicilian mafia, Calabrian 'Ndrangheta and Campanian camorra has a great number of similarities. Take the Sicilian mafia as an example, according to the description of a mafia informant Antonio Calderone:

> Cosa Nostra is the society of men of honor. According to estimates, these men number more than 1500, divided among 67 families in the province of Palermo alone. The families are the basic units each holding sway over a recognized territory. Each family has a chief, its capofamigila,

[10] Ibid, p.70.

chosen by its members. He is aided by a hand-picked consiglieri or counselor. Below come a number of deputies, and below them what could be called sergeants of the organization-each one known as the copodecina (head of ten) in charge of five, ten, 20 or even 30 soldati, the rank-and-file soldiers. Above the families lies the high command. The capomandamento is the colonel responsible for three families. He, in turn, answers to a provincial committee. Above that lies a regional committee, the government of the Cosa Nostra. Not even the Mafia claims national power. Instead, it has given affiliated membership to the heads of both the Calabrian' Ndrangheta and the Neapolitan Camorra.[11]

Base on the short introduction of the development of Italian mafia, some certain crucial elements and recurring features are also concluded as: the ongoing "violent modernization' of Sicily's politics and economy; the strained relations between the Italian state and Sicilian society; the frequent exercise of organized violence; and the presence of "violent entrepreneurs' aiming to control the main sources of income.[12] Italian mafia can be said to be a type of organized crime with "something extra", which resides in its organizational dimension-formal and secret, independent and pre-dating the management of single activities and illicit enterprises, and which operates as a primary element of internal identification and of defense against the outside. These common elements of Italian mafia can be concluded on the detailed archive research conducted by several historians (Pao Pezzino, Rosario Mangiameli and Salvatore Lupo) and the statements of mafia defectors turned government witnesses.[13]

1.2 Russia

[11] See Lyman et al., 2000:338, cited in Sean Grennan and Marjie T. Britz, *Organized Crime: a Worldwide Perspective*, Pearson Education, Inc.,Upper Saddle River, New Jersey, 2006, p.32.

[12] Gianluca Fulvetti, The Mafia and the "Problem of the Mafia": Organized Crime in Italy, 1820-1970, In Cyrille Fijnaut and Letizia Paoli (ed.) (2004), *Organized Crime in Europe: Concepts Patterns and Control Policies in the European Union and Beyond*, Springer, p.70.

[13] Gianluca Fulvetti, The Mafia and the "Problem of the Mafia": Organized Crime in Italy, 1820-1970, In Cyrille Fijnaut and Letizia Paoli (ed.) (2004), *Organized Crime in Europe: Concepts Patterns and Control Policies in the European Union and Beyond*, Springer, p.50

The development of Russian organized crime has been much faster than in other countries. Between the late 1950s and the end of the 1970s the social base of OC in Russia widened considerably, which was due to the appearance of a plurality of shadow economy entrepreneurs. Some Russian OCGs accumulated a great amount of wealth and cooperated with high-level party and government officials. These shadow economy entrepreneurs were usually obliged to accept the protection of the thieves-in-law, because most of their activities were considered illegal by the Former Soviet State.[14] From the end of the 70s of the last century onwards the rise of a new generation of criminals and more general consolidation of contemporary OC can be observed. Its criminal activities were initially related to traditional black-market drugs racketeering, arms and weapons dealing, and control over the gambling and sex businesses.[15] Apart from the two former stages, one prominent phase should be noted, from the middle of the 1980s onwards, Russian organized crime, in just 20 years, experienced the "western model" of organized crime, the "western model" which took more than one hundred years in western society. Another point which should be also emphasized is that the influence of contemporary Russian organized crime on the economy and state politics was also formed during this period. By the end of the 1990s, the implosion of the Soviet Union and the liberalization and democratization process created immense opportunities for the mergence of organized crime with legal business and political structures. From the time of former Soviet Union, ethnic organized criminal groups have been a notable feature of Russian organized crime, and they often monopolies certain types of crime in a particular area, taking Moscow as an example, Tajiks and Uzbeks of organized criminal associations engaged in drug business; Georgians organized criminal groups engaged in burglary; Kazakh OCGs engaged in fraud. Of course, the illegal activities of Russian organized crime also include trafficking in people and immigrants, sex and

[14] Yakov Gilinskiy and Yakov Kostjukovsky, From Thievish Artel to Criminal Corporation: the History of Organized Crime in Russia, In Cyrille Fijnaut and Letizia Paoli (ed.) (2004), *Organized Crime in Europe: Concepts Patterns and Control Policies in the European Union and Beyond*, Springer, p.183.
[15] Ibid, p.183.

pornographic businesses, arms and weapon dealing, and so on. According to the statistics of the Russian Federation Ministry of the Interior, in 2010 Russian organized criminal groups and gangs carried out 21,200 serious crimes, and 9300 particularly serious organized crimes happened between January and June of 2011.[16] At present, a Russian organized criminal group has even penetrated into the State Duma of Russia. One officials of the Russian Carnegie Foundation, Mike Faure said the Russian organized criminal groups vainly attempted to infiltrate in the State Duma to create a political network for their illegal activities.[17] Generally speaking, the level of development of Russian organized crime already endangered Russian national security. The president of Russia, Putin considered OC as one of the uppermost threats to national security in the "Formulation of National Security" in 2000.[18]

1.3 Germany

Relatively speaking, the step of German organized crime was a little slower than in Italy and other countries'. Until the 1960s and 1970s, a fierce debate concerning whether OC as the type of Italian mafia existed in Germany or not was still being launched between academics of Criminology and criminal law enforcement.[19] However, during the 1980s, especially in the 1990s it was generally recognized that Germany had OC. The reunification of Germany brought a fundamental revolution of social systems and structure, which led to a series of consequences, such as the surge of unemployment, inflation and social unrest. All of these factors provided German organized crime with

[16] Xu Kai. (2011). the Characteristics of Organized Criminals of Russian in 21C, Journal of Heilongjiang Administrative Cadre Institute of Politics and Law, Sum No.93.
[17] Mike Faure, Russia joins hand with the United States fighting against Mafia, Message posted to http://news.fm365.com/guoji/20000921/145932.htm.
[18] Putin, "Formulation of National Security" in 2000 of Russia. Cited in Xu Kai. (2011). the Characteristics of Organized Criminals of Russian in 21C, Journal of Heilongjiang Administrative Cadre Institute of Politics and Law, Sum No.93.
[19] Tao Ye, Study on Comparison of Organized Crime in The EU and China, 2007, P19.

ideal opportunities. As for the illegal activities of German organized criminal groups, they are involved in drug trafficking, sex and pornographic business, extortion, theft, robbery, forgery of bank notes, arms trafficking and other illegal fields. The sex business is the most rampant among illegal businesses of German organized crime. Since German up-market cars are very welcome in other regions of the world, car theft, committed by OCGs, is also serious in Germany. Apart from the former mentioned illegal activities, drug trafficking in Germany is also a serious crime. The drug organized criminal groups usually occupy some big cities as the main venues for their crimes, such as Berlin, Hamburg, Cologne, Frankfurt, Stuttgart and Munich. Now, Germany had become a haven for organized crime, even the Italian mafia who operate drug networks in America also use Germany to escape punishment and carry out money laundering.[20]

1.4 Austria

Austria is situated in the centre of Europe; this means the OCGs of Austria can connect with organized criminal groups of Italy, Russia, Eastern Europe and Central Asia. Maximillian Edelbacher has also pointed out those Austrian organized criminal groups[21]: OCGs of Former Yugoslavians, Serbs, Croats, Bosnians, Kosovo-Albanians, Turks, Iranians, Italians, Russians, Bulgarians and Chinese Mafia constitute OCGs which are active in Austria.[22] The local OCGs engage in procuring, gambling, bank robbery, burglary, handling stolen goods, fraud, forgery and cooperating with the Eastern neighboring countries in the name of "joint ventures".[23] former Yugoslavs, Serbs,

[20] Xu Jieqing, (2006), *A Study of Organized Crime in Taiwan District and the Countermeasures*, Chinese Procuratorial Press, p.53.
[21] They refer to the local organized criminal groups in Austria.
[22] Maximilian Edelbacher, Organized Crime in Austria-Vienna: The Gateway to the East. In *Organized Crime: A World Perspective*, Third International Police Executive Symposium, Kanagawa University, Yokohama, Japan Nov 28-Dec 1, 1996, The Society of Law, University of Kanagawa, Vol.31, No. 3, 1997, p.327-328.
[23] Ibid, p.327.

Croats, Bosnians, Kosovo-Albanians are involved in organized burglary, car thefts, drug and arms dealing.[24] The Turks and Iranians engage in drug trafficking.[25] Italians, Russians and Bulgarians are active in the area of bank robbery, underhand selling of cars and smuggling of people.[26] The so called "Chinese Mafia" are involved in the illegal activities of trafficking in human beings, extortion of protection fees, money laundering and drug dealing.[27] During recent years, the OC in Austrian is also developing with the coming of modern ICTs.[28] The OCGs use the internet to carry out almost all kinds of crimes.[29]

According to the Österreiche Sicherheitsbericht from 2006 to 2013, the quantities of organized associations and OCGs each year from 2003 to 2013 is indicated by table 1.[30] It reveals that from the police criminal statistics the number of OCGs in Austria declined year by year between 2003 and 2013. On the one hand, the Austrian Security Reports between 2006 and 2013 indicate that Austrian organized crime has a close relationship with OC in the Balkans, Turkey, Asia, Eurasia, Western Europe, America and Oceania. Different OCGs are involved in different illegal activities: Balkan organized criminal groups mainly carry out robberies, drug trafficking and property crimes; Turkish organized crime groups continue to carry out drug trafficking, arms trafficking, smuggling and extortion and increasingly economic crimes. The trend of cooperation between Turkish organized criminal groups and other ethnic criminal groups is increasing; Asian criminal groups usually operate in secret within their own Ethnicity, and usually these offenses are rarely made public, because both witnesses, victims avoid contact with the police. Their main fields of activity are smuggling, drug

[24] Ibid, p.327.
[25] Ibid, p.328.
[26] Ibid, p.328.
[27] Ibid, p.328.
[28] ICTs means Information Communication Technologies
[29] See the Cybercrime Repot of Austria 2012.
[30] Österreiche Sicherheitsbericht 2013, retrieved on 15. June.2015 from http://www.bmi.gv.at/cms/bmi_service/start.aspx#t_download.

trafficking, extortion and economic and financial offenses; Eurasian criminal groups mainly come from Georgia, Moldova and the Russian Federation, particularly from Chechnya. These groups are mainly involved in burglaries and theft and commercial transactions. By far the largest proportion of Eurasian criminal groups are now Chechen groups, which are active in all areas of crime, mainly in organized thefts, burglaries, robberies, vehicle movements, trafficking of narcotic substances and smuggling; Criminal organizations from Southern Europe are mainly characterized by a high degree of hierarchical structure. The territories controlled by Mafia groups include financial markets, political agitations, undermining and steering the Management to internal law. On the other hand, the Austria Security Reports between 2006 and 2013 reveals that the organized criminal groups began to commit crimes via the internet,[31]these reports also depict a fact that the offenders of cybercrime not only commit ICTs crimes but also traditional crimes, for example, carrying out online fraud, child pornography, extortion, property crimes, organized crime, smuggling and trafficking in human beings. These two aspects indicate a trend that OC is increasingly combined with cybercrime.

Table 1[32]: Development of reports on § 278 and § 278a since 2003

	§ 278StGB	§ 278aStGB
Year 2003	58	131
Year 2004	50	159
Year 2005	108	126
Year 2006	86	70
Year 2007	85	58

31 Österreiche Sicherheitsbericht 2013, retrieved on 15. June.2015 from http://www.parlament.gv.at/PAKT/VHG/XXIV/III/III_00186/index.shtml

32 This table is cited from Österreiche Sicherheitsbericht 2013.

Year 2008	42	44
Year 2009	39	18
Year 2010	39	14
Year 2011	55	25
Year 2012	32	6
Year 2013	40	6

According to the Criminal Development of Austria between 2004 and 2013, the Cybercrime Report of Austria from 2004 to 2009, 2011 and 2012, the Bundeskriminalamt did not report many cybercrimes, but these reports paid more attention to cybercrime.[33] This reflects the trends of cybercrime, accordingly the relationship of OC organized crime and cybercrime is revealed by this trend, just as the Kriminalitätsentwicklung 2011 in Österreich said that the crimes are migrating to the internet (Verschiebung der Kriminalität ins Netz).[34] At the beginning of internet age, the OCGs of Austria took the internet and computer system as criminal objects, but during the recent several years, the OCGs do not only take the internet and computer system as criminal objects but also use them as criminal instruments and as a platform on to carry out their illegal activities.[35]

2. **Evolution of Asian organized crime**

33 See the Criminal Development of Austria between 2004 and 2013 and the Cybercrime Report of Austria of 2011 and 2012, retrieved on 28.Dec.2013 from http://www.bmi.gv.at/cms/BK/meldestellen/internetkrimina/start.aspx.
34 See Kriminalitätsentwicklung 2011 in Österreich.
35 See the Kriminalitätsentwicklung 2011 in Österreich and cybercrime report 2011 and 2013.

In Asia, China is a country with a vast territory, and since the new China was established its organized crime has developed for decades, they usually maintain close contact with the OCGs of its neighbors. Relatively speaking, Japanese organized crime has existed for more years than Chinese organized crime, the former has high-level and full-fledged structure. Comparatively, OC in China and Japan are typical models. In the following context the development of Chinese organized crime and Japanese organized crime will be briefly described in this part.

2.1 China

Chinese organized crime began to mushroom from the middle of the 1980s: its development can be divided into 3 phases, 1980s, 1990s and from 2000 onwards. During the 80s of the 20C, both of academic of criminology[36] and criminal law enforcement[37] hold that there was no type of mafia criminal group in China, meanwhile they consider that "criminal gang" is a relatively proper term to define Chinese organized criminal associations. Most scholars categorized criminal gangs at a relatively lower level of organized crime, but, by contrast, mafia groups are deemed as the highest level. Accordingly, the different level is considered as the paramount difference between criminal gangs and mafia groups.[38] When criminal gangs began to surge, a majority of researchers considered these criminal gangs only to have limited characteristics of mafia-like organized criminal groups, and the level of criminal gangs' development was not equal to the latter's. However, the prominent features of Chinese organized criminal gangs included the following aspects, improvement of the level of

[36] See Wan Hanbin, the Explanation of Chinese Criminal Law (the draft of amendment), cited in Lu Jianping.eds. *Comparative Study of Organized Crime,* Law Press China, 2004, P.173.

[37] Chen Xingliang, Organized Crime or Criminal Organizations-Rationalistic Thinking of the Criminal Organizations with the Underground Gang Characteristics, issued in the Compilation of Annual Theses of China Law Science Association of Criminal Law in 2002, p.1008-1013, cited in Lu Jianping eds. *Comparative Study of Organized Crime,* Law Press • China, 2004, P.40.

[38] Wang Li, Monographic Study of Organized Crime, People's Press, p.17.

organization, expansion of the scope of their criminal activities, diversification of their illegal activities, enhancement of their violence, and penetration into the economic field and official authority. Chinese criminal gang further developed in the following decade, i.e., the phase of the 1990s. On the one hand, the local criminal organizations speeded up their pace to evolve into mafia-style criminal groups. In this connection, one case should be noted, it is that the first Chinese mafia criminal group emerged in the Pingyuan district of Yunnan Province.[39] On the other hand, transnational organized criminal groups, for example, OCGs of Hong Kong, Taiwan and Macao began to filter into the mainland of China. Their main illegal activities are drug trafficking and trafficking in persons and immigrants.[40] Finally, in the last phase, after 2000, local Chinese OCGs have become much more fully-fledged than the former two decades, and this change is reflected in their structure, methods and means of their criminal activities. Apart from this, the further penetration of transnational criminal organizations provided local Chinese criminal gangs with advanced "knowledge". During this period, it can be said that both criminal gangs and mafia criminal groups coexist in contemporary Chinese society. As for the type of transnational organized crime in China, a Chinese scholar argued that there are three types in the mainland of China, respectively, input type of organized crime from abroad, collusive type between local and foreign organized criminal groups and output type.[41] However, Chinese organized crime should not be confined to these three types, as the local type should also be included in. In other words, there are four types of OC in China, i.e., local type, input type, collusive type, and output type: (a) Local type refers to the local organized criminal groups which originated from local areas of China and commit their criminal activities within the territory of China; (b) Input type indicates that foreign criminal groups directly commit crimes in Chinese territory, or organize the Chinese local criminals to expand their strengths, or target the objects within Chinese territory to commit crimes from outside

[39] Xu Jieqing, (2006), *a Study of Organized Crime in Taiwan District and the Countermeasures*, Chinese Procuratorial Press, P.73.
[40] Ibid, p.74.
[41] Lu Jianping eds. *Comparative Study of Organized Crime*, Law Press • China, 2004, P.138-143.

Chinese territory via the internet, email or other instruments;[42] (c) collusive type refers to Chinese domestic organized criminal groups and TOCGs who utilize all sorts of opportunities to jointly commit crimes; (d) Output type indicates that Chinese organized criminal groups commit organized crimes outside China. However, output type should be emphasized, since it has rapidly developed during recent years, this can be indicated by a great number of cases happed in Angola, Argentina and Venezuela. Mainly targeting those local overseas Chinese these output criminal gangs committed kidnap, robbery, extortion and trafficking in persons and immigrants.[43]

2.2 Japan

Japanese organized crime has been effectively operating throughout Japan for over 300 years.[44] At present, three main Japanese criminal gangs are Yamaguchi-Gumi, Sumiyoshi-Kai and Inagawa-Kai, and their "reputations" are on a par with the Italian mafia. Until after world war Ⅱ Bouryokudan was widely used to refer to the organized crime in Japanese academic community, and Bouryokudan is equal with organized crime and Yakuza in the Japanese society.[45] Yakuza has three origins, respectively, Bakuto, Tekiya and Gurentai. Bakuto are groups who sponsored illegal gambling parties within their territories and earned profits from their gambling guests.[46] Tekiya are groups who peddled and were street performers or who had proclivity to do so. They had their own spheres and temples or streets.[47] Gurentai emerged after World War II, but its members had been recruited by another Bouryokudan, after that it disappeared

[42] Ibid, p.139.
[43] On- line news (2013), Retrieved on 30.Mar.2013 from http://www.mps.gov.cn/.
[44] Sean Grennan and Marjie T. Britz, *Organized Crime: a Worldwide Perspective*, Pearson Education, Inc.,Upper Saddle River, New Jersey, 2006, p.303.
[45] Xu Jieqing, (2006), *A Study of Organized Crime in Taiwan District and the Countermeasures*, Chinese Procuratorial Press, p.65.
[46] Ayako Uchiyama, Changes of Boryokudan after Enforcement of the Anti-Boryokudan Law in Japan. In *Organized Crime: A World Perspective*, Third International Police Executive Symposium, Kanagawa University, Yokohama, Japan Nov 28-Dec 1, 1996, The Society of Law, University of Kanagawa, Vol.31, No. 3, 1997, p.467.
[47] Ibid, p.467.

from Japanese society.[48] After World War II, under the conditions of disorder of Japanese society and insufficient power of the Japanese police, after continuous competition, expansion and combination, Bakuto, Tekiya and Gurentai generally developed into three main Japanese criminal gangs, i.e., Yamaguchi-Gumi, Sumiyoshi-Kai and Inagawa-Kai. However, there is no clear relationship among Bakuto, Tekiya, Gurentai, Yamaguchi-Gumi, Sumiyoshi-Kai and Inagawa-Kai.[49] Since the 1950s, many social and economic problems emerged in Japanese society, Yakuza quickly gained control of newly created black markets. The criminal gang members then extended their illegal activities, including gambling, extortion, prostitution, labor racketeering and drug trafficking. These new criminal gangs, most of them consisting of delinquents known as "Chimpira" started to appear in Japan. Some of these new organized criminal gangs were also called "Gurentai" or "Seishonen-furyo dan". A significant amount of turbulent contention had happened between old and new criminal gangs. Eventually, the new groups were assimilated into either the Tekiya or Bakuto (U.S. Customs Service, June 1993).[50] In recent years, according to one assessment of the National Police Agency of Japan in 2004, there were approximately 44,400 members belonging to Yakuza.[51] An obvious which trend appeared in contemporary time, is that much closer connection had been established between Japanese Yakuza and foreign OCGs. For example, Yakuza cooperated with Shanghai criminal gangs, Fujian criminal gangs and North East criminal gangs of China to commit illegal entry and robbery. They worked together with Taiwan criminal gangs to carry out trafficking in arms. They also collaborated with Korean criminal gangs to commit drug trafficking.

3. **Evolution of North American Organized Crime**

[48] Xu Jieqing, (2006), *A Study of Organized Crime in Taiwan District and the Countermeasures*, Chinese Procuratorial Press, p.66-67.
[49] Ibid, p.65.
[50] Sean Grennan and Marjie T. Britz, *Organized Crime: a Worldwide Perspective*. Pearson Education, Inc., Upper Saddle River, New Jersey, 2006, p.307.
[51] Assessment of National Police Agency of Japan in 2004, cited in Xu Jieqing, (2006), *A Study of Organized Crime in Taiwan District and the Countermeasures*, Chinese Procuratorial Press, p.68.

In North America American, Canadian organized crime and the Italian mafia have deep historical roots, so the development of The United States' and Canadian organized crime is a model of North American organized crime. The evolution of The United States' and Canadian organized crime will be introduced in the following section.

3.1 The United States

Before the 1920s, most of American organized criminal gangs were disorderly crowds, and persistent and large-scale organized crime was rare at that time. American organized crime began to mushroom after the "prohibition" of 1917 was issued. During this time Irish, Jewish and Italian-American gangs mainly operated an underground wine market.[52] Since the 30s of 20C onwards, these criminal gangs started to become involved in legal businesses to gain new economic source. Because these gangs consisted of immigrants and were scattered in various urban areas, the structure of these gangs can be described as a Feudal patriarchal structure. Their activities can be divided into camouflage for legitimate businesses and totally illegal businesses. The former includes food production, catering and real estate transactions and so on. As for the latter, it includes gambling, illicit liquor, sex business and usury, etc. The movie, "the Godfather", is an accurate picutre of American organized crime in that period. The United States can be called an ethnical smelting furnace, in the decade of the 21C, there are many origins of American organized criminal groups. In accordance with ethnic root they can be categorized into six groups, respectively, La Cosa Nostra (LCN), Italian Criminal Enterprises (ICE), Columbian/South American Drug Trafficking Enterprises, Mexican Drug Trafficking Enterprises, Russian/Eastern European Criminal Enterprises

[52] Ibid, P.45.

and Asian Criminal Enterprises.[53] Accordingly, the activities of these OCGs can be categorized as three types, respectively, providing illegal services, providing illegal products and intervening in legal businesses.[54] According to a survey report of the United States Congress, organized crimes have become very wide-spread, furthermore, they weaken the American economic system and even endanger the national security of America.[55]

3.2 Canada

As a neighbor of The United States, Canada is also a country with a legal system based on English common law, so the evolution of Canadian organized crime has some similarities with America's. As the Criminal Intelligence Service of Canada (1996A) identifies outlawed motorcycle gangs and associations of criminals of various similar ethnic backgrounds to be the major visible organized groups of criminals within Canada.[56] CISC also categorizes major organized crime groups in Canada as Asian, Eastern European, Italian, Aboriginal, outlaw motorcycle gangs (particularly the Hell's Angels), and Columbian in composition. Scholars, such as Brodeur added Youth gangs, prison gangs, skinheads and militia-type groups to the CISC list.[57] Asian groups took preponderance at every level of the Canadian heroin trade, for example, according to the reports of CISC (1996A), Asian groups originating from the People's Republic of China (PRC) are responsible for an estimated 80% of large scale heroin shipments into Canada.

---

[53] Harald Otto Schweizer, et.al, Organized Crime: A U.S. Perspective. In Jay S. Albanese, Dilip K. Das and Arvind Verma. (eds). (2003) *Organized Crime: World Perspective*, Person Education, Inc., Upper Saddle River, New Jersey 07458.

[54] Jays. Albanbse and Anderson, Organized Crime in America, 3rd edition, 1996. Cited in Xu Jieqing, (2006), *A Study of Organized Crime in Taiwan District and the Countermeasures*, Chinese Procuratorial Press, p.46.

[55] The Codification Combat against Organized Crime Worldwide, edited by Ministry of Law in Taiwan district,1996, p9-10. Cited in Xu Jieqing, (2006), *A Study of Organized Crime in Taiwan District and the Countermeasures*, Chinese Procuratorial Press, p.46.

[56] Daniel J. Koenig, (1996), Follow the Money Enterprise Crime in Canada, In *Organized Crime: A World Perspective*, Third International Police Executive Symposium, Kanagawa University, Yokohama, Japan Nov 28-Dec 1, 1996, The Society of Law, University of Kanagawa, Vol.31, No. 3, 1997, p.208.

[57] Ibid, P.208.

The activities of Asian criminal groups also include white collar crimes, like money laundering, counterfeit cheque schemes, telephone toll and credit card fraud. Eastern European criminal groups are usually involved in a potpourri of illegal activities ranging from extortion, murder, international fraud, large scale theft to money laundering, and smuggling of drugs, cigarettes, weapons or automobiles. Ethnic Italian organized criminal groups prefer drug trafficking, gambling, smuggling, money laundering and extortion, either alone or in association with other criminal groups to commit these crimes. Columbian drug trafficking organizations still play a significant role in the Canadian cocaine trade and in multi-million dollar money laundering operations. Organized aboriginal criminal activities primarily involve contraband smuggling of liquor, tobacco, firearms, prostitution, drugs, crimes against persons and smuggling illegal immigrants between the United States and Canada. According to the report of CISC, OCGs are employing computer criminals to gain access to telecommunications system, data banks, credit profiles and other personal information.[58] The fact that Canadian organized criminal groups began to use ICTs in this report reveals a new trend, namely that organized crime has become involved with the internet.

4. **Evolution of South American Organized Crime**

In this part, Columbia is chosen as representative of South American, since Columbia is known worldwide for its illicit drug industry, and it is also one of the largest producers of coca, opium poppies, and cannabis, the organized crime in Columbia can be said to be representative of South America.

[58] CISC reports, cited in Daniel J. Koenig, (1996), Follow the Money Enterprise Crime in Canada, In *Organized Crime: A World Perspective*, Third International Police Executive Symposium, Kanagawa University, Yokohama, Japan Nov 28-Dec 1, 1996, The Society of Law, University of Kanagawa, Vol.31, No. 3, 1997, p.208.

Columbia has seen increasing problems from OC that began from the 1970s until now. The large scale of its drug trafficking activities and its immense fallout on its people have also made it become an important international concern. Columbia is the largest producer of cocaine, and accordingly, a majority of Columbian organized crimes are concerned with illicit drug trafficking. It is well known that there are three insurgent groups which are active in Columbia, namely, Revolutionary Armed Force of Columbia (FARC), National Liberation Army (ELN), and dissidents of the recently demobilized People's Liberation Army (EPL/D).[59] All of these groups now are also actively engaged in drug trafficking operations. Columbian drug trafficking criminal groups target the United States and Europe as their main markets, so at present, Columbia remains a significant supplier of cocaine to America and other international drug markets. In order to maintain their vested interests and extend their illegal activities, Columbian drug cartels support terrorist groups and are also involved in arms smuggling. In some cases these cartels even have gained access to political levers of state, and by means of infiltration and bribes they obtain illegal benefits. Obviously, the drug cartels of Columbia have become very powerful and resourceful. In recent years, drug trafficking cartels were even in alliance with guerrilla organizations, and this trend exacerbates Columbian drug trafficking organized crime.

5. Evolution of Australia Organized Crime

Since Australia is the biggest country in Oceania, and Australian organized crime has relatively complete structure, it can be said that Australian organized crime is the model for Oceania. This dissertation selects Australia as representative to reflect the development of Oceanian organized crime.

[59] Leonardo Jesus Ramirez Rirea, et.al, (2003), In Jay S. Albanese , Dilip K. Das and Arvind Verma. (eds). (2003), *Organized Crime: World Perspective*, Person Education, Inc., Upper Saddle River, New Jersey 07458, p.301.

Throughout the last quarter of the 20th Century, the subject of OC had been an issue at both political level and in the law enforcement community in Australia. From the late 1960s onward, drug importation and the consequent growth of criminal behavior related to the distribution of illegal drugs became a matter of significant community concerns.[60] One type of Australian organized criminal groups is called "bikie", the New South Wales (NSW) crime Commission reported 32 active groups and over 4,000 members nationwide, with a disproportionate number concentrated in NSW.[61] These groups include native gangs, for example, the Commancheros, the Rebels, the Coffin Cheaters, and the Gypsy Jokers, and foreign gangs, such as the Hell's Angels, the Outlaws, and the Bandidos. Other groups in operation include the Nomads and the Life and Death Gang. As for illegal activities, Australian biker gangs engage in a variety of traditional organized crime. They are involved in prostitution rackets, drug trafficking, auto theft and extortion.[62]

6. **Tendency**

The development of OC includes its past and present. Its present is substantially formed by its past and the contemporary actors. Based on an international perspective the evolution of OC helps us to understand its causes, its position in society and the present situation. Even though this section only makes a brief introduction about the development of organized crime in certain countries, the trends of OC can be generalized as following:

[60] John Broome, (2003), In Jay S. Albanese , Dilip K. Das and Arvind Verma. (eds). (2003), *Organized Crime: World Perspectives*, Pearson Education, Inc., Upper Saddle River, New Jersey 07458, p.336.
[61] These data are cited in Sean Grennan and Marjie T. Britz,(2006) *Organized Crime: a Worldwide Perspective*,(p.307), Pearson Education, Inc.,Upper Saddle River, New Jersey, p.125.
[62] Ibid, p.125.

- The activities of OC usually include legal and illegal businesses.
- At the high-level of OC, corruption and bribery are often accompaniments, for by means of corruption and bribery OCGs maintain and expand variety of their activities.
- Each country's OC not only have undergone a rapid process of internationalization but also positively carried out increasing cooperation and interaction with foreign criminal organizations.
- The proliferation of Information Communication Technologies (ICTs) and telecommunication in OCGs, such as computers and the internet have brought significant changes to OC, and these changes will continue to develop in the next years.[63]

Section 2 Traditional Definitions of Organized Crime and Definition of Cyber Transnational Organized Crime

As a form of joint crime, OC should be distinguished from the crimes which are committed by a single person or simple joint offenders, because the harmfulness of OC is more serious than the latter types of crimes. The most significant difference between these three types of crime committed by single criminals, simple joint offenders and organized criminal groups, is that there is no administrative structure existing in crimes which are committed by single criminal or simple joint offenders. Especially the simple joint offenders in collusion with one another, but they just commit one particular crime, after their targeted crime is completed, this alliance may be dissolved rather than existing over a long period. In order to research organized crime, it is necessary to provide the theory of criminal community with a reasonable definition of OC, since it is

[63] In the following chapter, this trend will be discussed in detail

also helpful and a basis for understanding concepts and extensions of TOC and CTOC. However, it is not easy to define a scientific concept for OC as, in contrast, the concept of OC has been controversial in worldwide academic circles and law enforcement for a long time.[64] There are two reasons for this difficulty, i.e., one is that researchers stood on different standpoints, the other is that OC has different manifestations in different country and historical periods which have different background of legislation.[65] Nevertheless, this section will discuss disputes concerning different definitions of OC that have been concluded by scholars, and regional and international organizations, and finally give a definition of CTOC which is held by this dissertation.

1. Different Concepts of Organized Crime

Worldwide, until now, there has been no consensus about the concept of OC at regional and international level, because each country has its own legal system and the complexity of OC further makes it difficult to give a common standard about the definition of OC. Notwithstanding, academic researchers and authorities of certain countries, regional and international organizations have never given up to define OC.

Criminologist, Donald R. Cressey's definition of OC is used by the Federal Bureau of Investigation of the United States: [66]

> An organized crime is any crime committed by a person occupying, in an established division of labor, a position designed for the commission of crime providing that such division of labor also

[64] Kang Shuhua, ed, *Current Organized Crime and the Counter-measures*,China Fangzheng Press, 1998, p.1. Cited in Lu Jianping eds. *Comparative Study of Organized Crime*, Law Press • China, 2004, P.10.
[65] Lu Jianping eds. *Comparative Study of Organized Crime*, Law Press • China, 2004, P.10.
[66]Donald R. Cressey, cited in Howard Abadinsky, (1990), *Organized Crime* (Third Edition), Nelson-Hall Inc, p.3.

includes at least one position of corrupter, one position for a corruptee, and one position for an enforcer.

As a criminologist, Donald R. Cressey's definition is concerned less with the criminal activities than with the perpetrators and the relationships among them. His definition has practical importance in law enforcement since it is used by the Federal Bureau of Investigation.[67]

Michael Maltz is also concerned more with the relationship of OCGs than the actual criminal behavior. He points out a problem of semantics: we call a specific behavior or act organized crime, but when we refer to OC in the generic sense, we usually mean an entitiy, a group of people. Thereof, he gave a "tentative" definition of OC,[68] and he is especially concerned with the dynamics of OCGs:

A crime consists of a transaction proscribed by criminal law between offenders(s) and victim(s). It is not necessary for the victim to be a complainant or to consider himself victimized for a crime to be committed. An organized crime is a crime in which there is more than one offender, and the offenders are and intend to remain associated with one another for the purpose of committing crime. The means of executing the crime include violence, theft corruption, economic power, deception, and victim participation. These are not mutually exclusive categories; any organized crime may employ a number of these means.

The objective of most organized crimes is power, either political or economic. These two types of objectives, too, are not mutually exclusive and may coexist in any organized crime.

There are a number of manifestations that objectives may take. When the objective is political power it may be of two types: overthrow of the existing order, or illegal use of the criminal

[67]Howard Abadinsky, (1990), *Organized Crime* (Third Edition), Nelson-Hall Inc, p.3.
[68] Michael Maltz, cited in Howard Abadinsky, (1990), *Organized Crime* (Third Edition), Nelson-Hall Inc, p.3.

process. When the objective is economic power, it may manifest itself in three different ways: through common crime (mala en se), through illegal business (mala prohibita or vices), or through legitimate business (white collar crime).

Michael Maltz's definition is much broader than Donald R. Cressey's. It relatively generalized the features of OC, such as criminal instruments, objectives and manifestations that objectives may take. But it did not clearly give the lowest number of offenders in OC.

Howard Abadinsky defined organized crime as: [69]

> Organized crime is a non-ideological enterprise involving a number of persons in close social interaction, organized on a hierarchical basis, with at least three levels/ranks, for the purpose of securing profit and power by engaging in illegal and legal activities. Positions in the hierarchical and positions involving functional specialization may be assigned on the basis of kinship or friendship, or rationally assigned according to skill, and the positions are not dependent on the individuals occupying them at any particular time. Permanency is assumed by the members who strive to keep the enterprise integral and active in pursuit of its goals. It eschews competition and strives for monopoly on an industry or territorial basis. There is a willingness to use violence and /or bribery to achieve ends or to maintain discipline. Membership is restricted, although nonmembers may be involved on a contingency basis. There are explicit rules, oral or written, which are enforced by sanctions that include murder.

Howard Abadinsky gives a definition of OC at a relevant higher level of organized crime. This type of OC with a hierarchical structure can be deemed as non-ideological enterprise. He further concluded 8 characteristics of OC and explained the meaning of

[69] Howard Abadinsky, (1990), *Organized Crime* (Third Edition), Nelson-Hall Inc, p.5.

them: (1) Nonideological, an OCG does not have political goals nor is it motivated by ideological concerns; its goals are money and power. While political involvement may be part of the group's activities, its purpose is to gain protection or immunity for its illegal activities. This distinguishes groups of persons who may be organized and are violating the law to further their political agenda from organized crime; (2) Hierarchical, an OCG has a vertical power structure with three or more permanent ranks, each with authority over the level beneath. The authority is inherent in the position and does not depend on who happens to be occupying it at any given time; (3) Limited or exclusive membership, an OCG has significant limitations on who is qualified to become a member, these may be based on ethnic background, kinship, race, criminal record, or similar considerations; (4) Perpetuitous, an OCG constitutes an ongoing criminal conspiracy designed to persist through time, beyond the life of the current membership; (5) Using illegal violence and bribery in an OCG. Violence is a readily available and accepted resource. Access to private violence is an important element that allows the group to remain viable and carry out its goals. When necessary, the OCG will resort to bribery in order to protect its operation or members. The use of violence or bribery is not restricted by ethical consideration, but is controlled only by practical limitations; (6) Demonstrates specialization/division of labor, an OCG will have certain functional positions filled by qualified members. Given the nature of an OCG, the position of enforcer is often crucial. This person carries out difficult assignments involving the use of violence. The enforcer may use members or non-members to accomplish the assignment. Less difficult assignments involving violence can be carried out by any member. The enforcer does not act independently but receives assignments, directly or indirectly, from the head of the OCG. If the group is sophisticated enough, it may also have positions for fixer and money mover. The fixer excels in developing contacts with criminal justice and /or political officials and, when appropriate, arranges for corruption. The money-mover is an expert at "laundering" illicitly obtained money, disguising its origin through a string of transactions and investing it in legitimate enterprises. Certain OCGs also have a position equivalent to intelligence analyst; (7) Monopolistic, an OCG

does not like competition. It strives for hegemony over a particular geographic area over a particular "industry," legitimate or illegitimate, or over a combination of both. An OC monopoly is maintained by violence, the threat of violence, or by corrupt relationship with law enforcement officials. A combination of these methods may be employed; (8) Governed by rules and regulations, an OCG, like legitimate organizations, has a set of rules and regulations which members are required to follow.[70]

Donald R. Cressey, Michael Maltz and Howard Abadinsky defined OC during the period of the 60s to the 90s of last century in the perspective of the USA. There are some points to be noticed concerning their definitions: Firstly, their definitions did not mention minimum members who comprise organized criminal groups; secondly, Donald R. Cressey and Howard Abadinsky discussed division of labor in OCGs in their definitions. In contrast, Michael Maltz did not mention it. Thirdly, as for the goals of OC, in Donald R. Cressey's definition the goals of organized crime are indefinite, they were described as a position designed for the commission of crime. Michael Maltz held opinion that the objective of most organized crimes is power, either political or economic, i.e., organized crimes are with nonideological or ideological goals rather than being restricted to material benefits or power; Finally, each of them does not clarify the subject aspect of OC, actually, organized crimes are intentionally committed instead of being committed by negligence.

Russian scholars, Yakov Gilinskiy and Yakov Kostjukovsky concluded OC as follows: [71]

[70] Ibid, p.5-8.

[71] Yakov Gilinskiy and Yakov Kostjukovsky, From Thievish Artel to Criminal Corporation: the History of Organized Crime in Russia, In Cyrille Fijnaut and Letizia Paoli (ed.) (2004), *Organized Crime in Europe: Concepts Patterns and Control Policies in the European Union and Beyond*, Springer, p.182 .

> Organized crime is the functioning of stable, hierarchical associations, engaged in crime as a form of business, and setting up a system of protection against public control by means of corruption.

Four attributes can be concluded from Yakov Gilinskiy and Yakov Kostjukovsky's definition: (1) division of labor is indicated by the term of "functioning of stable"; (2) hierarchical structure; (3) carrying out illegal activities; (4) by means of corruption against public control. This definition is not very precise, the reason can be analyzed at least from 3 points: Firstly, they did not clarify that OC must be committed with intention; Secondly, the goals of organized crimes were not detailed in this definition; Finally, a great number of cases indicate that not all organized crimes against public control are by means of corruption. Probably, corruption is often used in the highest level of organized crimes.

In some countries, in order to take action against organized crime, the state and federal governments had a clearly stipulated definition of organized crime in corresponding statutes. In the U.S, the state of Mississippi defined it as "Two or more persons conspiring together to commit crimes for profit on a continuing basis". Compared with this simple definition, the state of California's is more elaborated. It was described as "Organized crime consists of two or more persons who, with continuity of purpose, engage in one or more of the following activities: (1) The supplying of illegal goods and services, i.e., vice, loansharking, etc.; (2) Predatory crime, i.e., theft, assault, etc. Several distinct types of criminal activity fall within this definition of organized crime.[72] In Oregon the definition is "organized crime is a self-perpetuating, conspiracy operating for profit or power, seeking to obtain immunity from the law through fear and

[72] Howard Abadinsky, (1990), *Organized Crime* (Third Edition), Nelson-Hall Inc.

corruption".[73] In the United States, majority of states in America have their own concepts of organized crime.

Mississippi's definition is relative broader, it include five elements of OC, i.e., the minimum number of OCGs, conspiracy, committing crimes, striving for profits and continuity of operation. The definition of California relatively underlines the illegal activities which are committed by organized criminal groups. It touches on minimum numbers, continuity of operation and illegal activities of OCGs, but it does not discuss subjective aspect of organized crime. Compared with the former definition, attributes of Oregon's definition can be concluded as continuity of operation, conspiracy, striving for economic profit or power, seeking immunity through fear and corruption.

Comparedwith the U.S, most European states also made efforts to define the concept of OC. In Italy, the first law particularly addressing mafia, which was passed as early as May 1965, failed to specify what mafia meant, a specific offence of associazione a kelinquere di tipo fafioso (mafia-type criminal associations) was defined in 1982 by Act No.646. The bill modified the Criminal Code by introducing Article 416bis.[74] According to this provision, a mafia-type delinquent association consists of three or more persons, and

> Those who belong to it make use of the power of intimidation afforded by the associative bond and the state of subjugation and criminal silence which derives from it to commit crimes, to acquire directly or indirectly the management or control of economic activities, concessions,

[73] Arvind Verma, (1997), Organized Crime in India, In *Organized Crime: A World Perspective*, Third International Police Executive Symposium, Kanagawa University, Yokohama, Japan Nov 28-Dec 1, 1996, The Society of Law, University of Kanagawa, Vol.31, No. 3, 1997, p.116.

[74] Cyrille Fijnaut and Letizia Paoli, Introduction to Part 1: The History of the Concept, in Cyrille Fijnaut and Letizia Paoli (ed.) (2004), *Organized Crime in Europe: Concepts Patterns and Control Policies in the European Union and Beyond*, Springer, p.34.

authorizations or public contracts and services, either to gain unjust profits or advantages for themselves or for others.

The Italian official definition underlines the characteristics of mafia-type OCGs. Some elements of organized crime are indicated by it: (1) Using violence, like the power of intimidation or subjugation; (2) certain structure, it is revealed by the term of associative bond; (3) illegal activities; (4) striving for unjustly material profits or advantages. However, this definition does not touch on the subjective aspect of minimum numbers and perpetuation of organized crime.

In 1986 by the Ministers of the Home Affair and Justice of the German federal states agreed on a common definition of OC as follows[75]:

Organized crime constitutes the planned commission of criminal offences driven by the quest for acquiring profits or powers. Such criminal offences have to be, individually or in their entirety, of major significance and involve the cooperation of more than two participants acting with a common intent for a longer or indefinite period of time on a distributed-task basis

a) By utilization of commercial or business-like structures;

b) By application of violence or other methods suitable for achieving intimidation; or

c) By exerting influence on politics, the media, public administrations, justice systems, or commerce and industry.

The German official definition gives the elements of OC as follows: (1) illegal activities; (2) acquiring profits or power; (3) minimum number more than two parictipants; (4)

[75] Gemeinsame Richtlinie der Justizminister/-senatoren und der Innenminister/-senatoren der Länder über die Zusammenarbeit von Staatsanwaltschaft und Polizei bei der Verfolgung der Organisierten Kriminalität, published in Kleinknecht and Meyer-Goßner (2001), *Richtlinien für das Straf-und bußgeldverfahren* (RiStBV), Anlage E, Punkt 2.1. Jörg Kinzig and Anna Luczak, Organized Crime in Germany: A Passe-Partout Definition Encompassing Different Phenomena. Cited in Cyrille Fijnaut and Letizia Paoli (ed.) (2004), *Organized Crime in Europe: Concepts Patterns and Control Policies in the European Union and Beyond*, Springer, p.335.

common intention; (5) perpetuitous; (6) commercial or business-like structure; (7) using violence or other methods.

The Austrian definition of organized crime can be found in the Criminal Code of Austria, the § 278a StGB is the provision that concern the definition of OCG, it was called "Kriminelle Organization"[76]:

> Establishing an organization that is composed of multiple people and carries out illegal penalizable activities during a long period, or participating in this organization as its member,
>
> 1. This criminal organization repeatedly planned to commit serious crimes that must be penalized, such as targeting at life, body integrity, freedom, property or carrying out sexual exploitation, prostitution medium, trade in arms without license, nuclear material, radioactive material, dangerous waste, counterfeit currency addictive substances,
> 2. This criminal organization seeks to obtain huge illegal interests, and
> 3. This criminal organization avoids prosecution and criminal penalty via corruption, intimidation or other ways, all of these behaviors should be punished with imprisonment from six months to five years according to 278 Abs. 4.

From this description, some elements of definition of OC in Austria can be generalized: （a）Organized crime in Austria must be carried out by business-like criminal organizations;（b）This criminal organization must be composed of at least 10 people;（c）this criminal organization must exist for a long period of time;（d）The aims of the criminal organization are to carry out illegal penalizable activities; (e) The goal of criminal organizations is to obtain the maximum material benefit.

[76] See §278a StGB of Criminal Code of Austria.

The National Criminal Intelligence Service (NCIS) in the United Kingdom in its annual assessment of the threat of organized crime for 2000 gave some certain criteria to define the concept of OC: a criminal group should contains at least three persons; they engage in criminal activity that is prolonged or ongoing; their members are motivated by profit or power; they commit serious criminal offences (NCIS, 2000).[77]

In China (mainland), the concept of OC is just discussed and disputed in the academic community. At legislation level, the authority of China adopted the term of underground groups rather than mafia-type groups to define Chinese organized criminal group. They argued that mafia-type crimes are still rare in China. Even though the authorities hold such perspective, most scholars consider that int recent years OC has merged and developed rapidly in China. A majority of scholars also argue that the definition of OC can be concluded as: Organized crime is committed by OCGs, they consist of three or more persons, and in order to commit one or more crimes, these groups exist in a given period. They engage in legal economy and politic to gain economic profits and power. In contrast with those definitions of scholars, the Standing Committee of the National People's Congress adopted "Explanation of the item 1of article 294 of Chinese Criminal Code" on 28 April of 2002, it describes 4 characteristics of OCGs as follows:[78]

1. A stable criminal organization has been established, this organizations includes certain members, is fixed with specific organizers and leaders who are stable in organized criminal groups;

2. By means of committing criminal activities or other instruments to gain economic benefits, with certain economic power for supporting their activities;

[77] Letizia Paoli and Cyrille Fijnaut (2004), In Cyrille Fijnaut and Letizia Paoli (ed.) (2004), *Organized Crime in Europe: Concepts Patterns and Control Policies in the European Union and Beyond*, (p.36), Springer.
[78] See "Explanation of the item 1of article 294 of Chinese Criminal Code" 0f Standing Committee of the National People's Congress on 28 April of 2002, it is legislative explanation of criminal law

3. Repeatedly commit crimes by means of violence, intimidation and other instruments, these cause damages to other citizens;

4. Establishing illegal control or exerting notable influence via committing criminal activities or utilizing the shield and connivance which are provided by state personnel, these illegal activities seriously harm the order of economy and social life;

There is no available official definition in Chinese criminal law or other related laws, but the former legislative explanation provides practice with the four characteristics of organized crime. In view of this explanation, elements of organized crime in China can be concluded as: (1) certain structure; (2) committing illegal activities; (3) striving for material benefits or power; (4) using violence or other methods. However, one point need to be underlined, it is that the shield and connivance which are provided state personnel are not necessary for OC in China.

At regional level, the European Union has been considering a definition of OC based on eleven characteristics:

1. Collaboration of more than 2 people;

2. Each with own appointed tasks;

3. For a prolonged or indefinite period of time;

4. Using some form of discipline and control;

5. Suspected of the commission of serious criminal offences;

6. Operating on an international level;

7. Using violence or other means suitable for intimidation;

8. Using commercial or businesslike structures;

9. Engaged in money laundering;

10. Exerting influence on politics, the media, public administration, judicial authorities or the economy;

11. Determined by the pursuit of profit and/or power.

Among these characteristics, in accordance with concept of organized crime, at least six of them must be satisfied, three of which must be those number 1, 5 and 11.[79]

At international level, in 2001 Edelbacher cited the definition of the International Criminal Police Organization (Interpol) which describes OC as a "systematically prepared and planned committing of serious criminal acts with a view to gain financial profits and power…by more than three accomplices united in hierarchy and job divisions...in which the methods of violence, various types of intimidation, corruption and other influences are used".[80] As the aspect of defining OC, the United Nations has eschewed the approach of identifying the characteristics of OC, it prefers to not face the difficulty of defining organized crime. The United Nations Convention against Transnational Organized Crime (UNTOC) has basically resolved to combine a generic definition followed by a number of conventions that aim to criminalize certain activities. Such as definitions of illicit traffic in narcotic drugs or psychotropic substances, money laundering, trafficking in persons and counterfeiting currency. The definition of organized crime is defined as: Organized crime means group activities of three or more persons, with hierarchical links or personal relationships which enable their leaders to

[79] 6204/1/97 (ENFOPOL 35 REV 2) DG H Ⅱ, in the Annual Report of European Union concerning Organized Crime.

[80] Jay S. Albanese and Dilip K. Das (2003). In Jay S. Albanese , Dilip K. Das and Arvind Verma. (eds). (2003), *Organized Crime: World Perspective*, Pearson Education, Inc., Upper Saddle River, New Jersey 07458, p.5.

earn profits or to control territories or markets, internal or foreign, by means of violence, intimidation or corruption, both in furthering criminal activities and infiltrating the legitimate economy (M.Cherif Bassiouni and Eduardo Vetere, 1998).[81] There is no doubt that the UNTOC can be considered as the most important attempt to arrive at a global consensus about the definition of organized crime. UNTOC applies to serious crimes that are transnational in nature and involve OCGs, such as corruption, money laundering, drug trafficking and obstruction of justice, etc. However, it just defines the concepts of an organized criminal group, serious crime and structure group instead of explicitly stipulating the concept of OC or TOC. According to article 2 of UNTOC:[82]

a) "Organized crime group" shall mean a structured group of three or more persons, existing for a period of time and acting in concert with the aim of committing one or more serious crimes or offences established in accordance with this convention, in order to obtain, directly or indirectly, a financial or other material benefit;

b) "Serious crime" shall mean conduct constituting an offence punishable by a maximum of at least four years imprisonment or a more serious penalty;

c) "Structured group" shall mean a group that is not randomly formed for the immediate commission of an offence and that does not need to have formally defined roles for its members, continuity of its membership or a developed structure

It is a pity that UNTOC only defined some related definitions instead of defining organized crime. Undoubtedly, a clear definition of organized crime can provide the state parties of UNTOC with a guide for implementing UNTOC and its protocols.

[81] M.Cherif Bassiouni and Eduardo Vetere, (1998), Towards Understanding Organized Crime and Its Transnational Manifestations, M.Cherif Bassiouni and Eduardo Vetere, (eds), In *Organized Crime: A Compilation of U.N. Documents 1975-1998*, Transnational Publishers, Inc.

[82] See The United Nations Convention against Transnational Organized Crime, retrieved on 26 July 2013 from https://www.unodc.org/unodc/en/treaties/CTOC/index.html?ref=menuside.

Most of the aforementioned concepts of OC reveal some its core elements, such as a certain number of members, organized structure, existing over a certain lengthy period, carrying out illegal activities, striving for material benefits or power. These elements are important to OC, the reasons include: firstly, a certain number of members can distinguish OCGs from the crimes which were committed by a single perpetrator; secondly, organized structure and a long period can differentiate OC from the crimes which were committed by simple joint offenders;[83] thirdly, carrying out illegal activities draws a clear line between OCGs and legal associations or organizations; finally, the members of OCGs who organize together to commit crimes in a long period of time must aim at goals of material benefits or power.[84] Of course, these elements are expected in the past historical context. However, in the information age, we need to adjust our perspective during the process of defining OC. For example, in those organized crime committed via the internet, it is possible that the offenders never know each other in the real world. Accordingly, it is also possible that there is no hierarchical structure within some cyber organized crimes. Some organized criminal groups' structure in the era of internet is like a net, the criminals are the nodes of this net, and the internet is its thread. For example, online news from the official website of the Ministry of Public Security of the People's Republic of China,[85] covered the illegal activities of dealing in individuals' personal information via the internet, which were committed by OCGs. The structure of these crimes is comprised of three levels, i.e., origin of individuals' personal information[86], platform of data[87] and illegal investigation enterprises[88]. According to this coverage, buyers and sellers of these deals contacted each other by the internet rather than face to face in the real world, so they did

[83] The simple joint crime means that the criminals organized together to commit one crime, and there is no demonstrated specialization between them.

[84] this dissertation is with the standpoint that the goals of organized criminal groups are not just limited as material benefits or power, which will be discussed in the part of The definitions of organized crime in the Era of Internet.

[85] Online news, retrieved on 27 July 2013 from http://www.mps.gov.cn/n16/n1237/n1342/n803715/3224583.html.

[86] Some of the staffs who work in certain state organs, enterprises or service organizations, can directly contact thepersonal information of citizens, and they are the source of individuals' personal information.

[87] Middlemen established the platform of data via internet, they directly get the citizens' personal information, after that they sell them between themselves or to other person and organizations.

[88] The illegal investigation enterprises committed downstream crimes after they bought citizens' personal information from the middleman.

not know each other's real identity in the real world. Obviously, the structure of these crimes is different from the hierarchical structure of OC before internet age. But beyond all doubt, these traditional concepts provide us with guidance when defining the concept of CTOC.

2. Definitions of Organized Crime in the Era of the Internet

In accordance with the above mentioned concepts of OC, some of them can accurately reveal the phenomenon of OC before the internet age. However, these definitions also have weaknesses. Some of them are too narrow: Firstly, as for the narrow ones, taking Donald R. Cressey's definition as an example, he defined OC as at least including one position of corrupter, one position for a corruptee and one position for an enforcer. However, the fact is that not every organized crime has a position of corrupter and corruptee; Secondly, in the majority of the aforementioned definitions, the goals of organized crime were set within the confines of material benefits or power, which means that an OCG is motivated neither by political goals nor by ideological concerns;[89] Thirdly, some definitions also argued that an OCG must have a hierarchical structure. Obviously, this is does not tally with the factual situation of OCGs in the internet era. Thereof, in the internet age, some elements of OCGs and OC need to be slightly adjusted to match up to the evolution of organized crime. This part tries to define OC in the era of the internet, in other words, how to reasonably define OC. Even though there is no consensus on the definition of OC among scholars and law enforcement agencies, some core elements can be identified from the definitions of most state statutes and scholars. Undoubtedly, these provide foundations for a definition of OC, TOC and CTOC. Base on these core elements this dissertation tries to define OC in the era of the internet, i.e., CTOC

[89] See Howard Abadinsky' definition.

In order to accurately grasp a definition of OC, the first step is that it is necessary to take into account the particular context and changes when analyzing OC. In accordance with this standard, the context includes particular legal and historical background. So at this level, in order to properly reveal the phenomenon of OC, the definition of OC should be dynamic rather than fixed. In other words, in accordance with its era, the concepts of OC in different historical periods should be a generalization of the true situation of organized crime. Secondly, among these core elements of organized crime, two categories should be distinguished, respectively, mandatory attributes and optional attributes. Just as the table 2[90] shows in the following：

Table 2: core elements of cyber transnational organized crime

Mandatory attributes	Optional attributes
1. Collaboration of three or more persons 2. For a prolonged or indefinite period of time 3. Intentionally or deliberately committing crimes with common intent (subjective aspect of organized crime) 4. Committing illegal activities 5. With the goals of pursuing profit	1. Having a specific task or role for each participant 2. Using some forms of internal discipline and control 3. Using violence or other means suitable for intimidation 4. Exerting influence on politics, the media, public administration, law enforcement, the administration of justice or the economy by corruption

[90] This table is made base on Organized Crime Situation Report 2004: Focus on the Threat of Cybercrime, which was issued by Council of Europe-Octopus Programme.

and/or power, or the other non-material interests (e.g. political purpose) 6. At least two or more countries are involved 7. Targeting the internet or internet-related devices, or the internet is used as the instruments	or any other means 5. The protection of the authorities of states 6. Using hierarchical, commercial or business-like structures 7. Engaged in money laundering

In the following text, this article names these attributes as M (1) or O (1), et cetera. The reasons why this dissertation distinguishes these attributes should be detailed as: M(1) can differentiate CTOC from cyber transnational crimes which are committed by two offenders; M(2) means the perpetuation of CTOC, it separates them from the simple joint criminal gangs which just commit one particular crime or some certain number of crimes; M(3) indicates that CTOC must be premeditated crimes, they are intentional or deliberately committed; M(4) means that illegal activities are the main activities of cyber transnational organized crime; M(5) indicates that CTOC strives for material profits, power or the other non-material benefits, these benefits and power can support their continuity and perpetuation; M(6) indicates that CTOC is international crime; M(7) distinguishes CTOC from TOC before the internet age. As for the Optional attributes, they are concluded from the aforementioned definitions before the internet age, and they are not necessary for CTOC.

Among the mandatory attributes, M (1), M (2) and M (4) should be emphasized. M (1) adopts the opinion that the minimum number of CTOC should be three or more persons

instead of two or more persons[91], since the case of two criminals committing crimes should be deemed as simple joint crime. Undoubtedly, M (2) reveals that the commission of crimes with common intent is simply joint crimes the criminal alliance will be dissolved after the crime is finished, which means there is no complicated organized structure among the criminals. As for M (4), this article holds that the goals should not be restricted to financial profits and power, political aims or other non-material goals, but should also be included in the goals of CTOC. This dissertation argues that cyber transnational terrorism organized crime is one type of CTOC, cyber transnational terrorism groups are also a subordinate concept of cyber transnational organized criminal groups (CTOCGs), for reasons which can be concluded as follows: (1) it is probable that CTOCGs purely strive for material benefits or power. However, in practice, they and cyber transnational terrorism groups can overlap, even transform into each other; (2) the goals of them are the only difference between CTOCGs and cyber transnational terrorism groups, some of CTOCGs pursue material profits or power, in contrast to cyber transnational terrorism crimes seeking to achieve certain political goals. The goals of cyber transnational terrorism groups are not the elements which pick them out from CTOCGs.

Based on the above analysis of attributes of CTOC, its definition can be concluded as: cyber transnational organized crime is any crime intentionally or deliberately committed by three or more persons with common intent, in order to pursue material profits, power or the other non-material interests. In order to commit more crimes instead of one crime, the members of these groups are combined with each other in a prolonged or indefinite period of time, and by means of ICTs these crimes targeting internet or internet-related devices, or the internet is used as the instruments to commit crimes, with at least two countries involved. That is the meaning of transnational.

[91] The definition of the state of Mississippi in U.S

Conclusion of Chapter 1

This chapter analyzes the history of organized crimes and its definitions in the past with an international perspective. Firstly, the history of OC provides us with a background for understanding the original relationship between CTOC and OC. Secondly, by means of introducing definitions of organized crime at international level, we can be fully aware of the common attributes of organized crime in its history. Further compared with present CTOC, on the one hand, those attributes that already can not reflect OC in the internet age have been discarded. On the other hand, new attributes that meet the criterion of CTOC have been supplemented into the concept of CTOC. In view of these two steps, at the end of this chapter, a definition of CTOC, which is proposed by this dissertation, is set out. It will supply a basis of understanding the new changes of OC in the context of the internet.

Chapter 2 Characteristics and New Trends of Organized Crime in the Era of the Internet

The first chapter analyzes the history and definition of organized crime, and concludes the definition of CTOC finally. Accordingly, this chapter will concentrate on analyzing the combination of organized crime and cyber crime, in other words, new changes and trends of organized crime in the internet age. At present, it is well known that both organized crime and cybercrime are some of the greatest challenges in the 21st century. So if they overlapped or converged with each other, nobody knows how many complex problems would be brought to our civil society. One fact is that they have been merging with each other since the internet and the other ICTs entered our daily life; the combination of organized crime and cybercrime creates new manifestations of organized crime, and it is named as cyber transnational organized crime in this dissertation. In the light of this new development of organized crime, in order to conclude the present characteristics and new trends of organized crime in the era of the internet, certain cases are studied in this chapter.[92]

Section 1 Characteristics of Present Organized Crime

A recent report stated that victims lose around €290 billion, as a result of cybercrime, each year worldwide, which makes it more profitable than the global trade in marijuana, cocaine and heroin combined.[93] Undoubtedly, substantial material profits are definitely a tremendous temptation to the transnational OCGs. Obviously, the convergence of TOC and cyber crime has been proved by substantial facts, which will be demonstrated

[92] The internet in this dissertation includes any devices which can access to it, such as computers, smart phones and so on.

[93] Cybercrime: A Global Growing Problem, Retrieved on 03.Aug.2013 from https://www.europol.europa.eu/ec/cybercrime-growing.

via case study. The following 250 cases, collected from official websites at random, concerning OC relating to the internet between May of 2003 and July of 2013 will be studied. These official websites include the FBI[94], the Ministry of Public Security of the People's Republic of China[95], RCMP (Royal Canadian Mounted Police)[96], AFP (Australian Federal Police)[97], SOCA (Serious Organized Crime Agency of the UK)[98], Interpol (International Criminal Police Organization)[99], Sina net[100] and Xinhua net[101]. All of these cases, associated with the internet, were selected from these 8 official websites. Many countries were involved in these cases. The origins of these cases can be revealed by table 1and table 2, 3, 4, 5, 6 and 7.[102]

Table 1: the sources of pending cases

Source	Quantity :250
America: http://www.fbi.gov/	28
China: http://www.mps.gov.cn/	188
Canada:http://www.rcmp-grc.gc.ca/index.htm	1
U.K: http://www.soca.gov.uk/	10
Australia: http://www.afp.gov.au/default.aspx	14
Interpol: http://www.interpol.int/	4
Sina net: http://news.sina.com.cn/	1

[94] See http://www.fbi.gov/.
[95] See http://www.mps.gov.cn/.
[96] See http://www.rcmp-grc.gc.ca/index.htm.
[97] See http://www.afp.gov.au/default.aspx.
[98] See http://www.soca.gov.uk/.
[99] See http://www.interpol.int/.
[100] See http://news.sina.com.cn/.
[101] See http://news.xinhuanet.com/world/.
[102] These tables are made by the author of this dissertation, and because the following analysis is based on information from these 250 cases, it is impossible to specify all the details of these cases, so it cannot be particularly indicated where they are used as a reference. However, table 2 can indicate the original sources of these cases.

Xinhua net: http://news.xinhuanet.com/world/[103]	4

Table 2: the original sources from America

1	On-line news, Retrieved on 30.June.2013 from http://www.fbi.gov/losangeles/press-releases/2012/armenian-power-member-and-three-armenian-power-associates-convicted-in-los-angeles-for-roles-in-identity-theft-ring
2	On-line news, Retrieved on 30.June.2013 from http://www.fbi.gov/news/stories/2012/march/predators_030112/predators_030112
3	On-line news, Retrieved on 30.June.2013 from http://www.fbi.gov/newhaven/press-releases/2012/alleged-organized-crime-associates-among-20-charged-with-operating-illegal-gambling-businesses-in-connecticut
4	On-line news, Retrieved on 30.June.2013 from http://www.fbi.gov/news/stories/2012/april/grandparent_040212/grandparent_040212
5	On-line news, Retrieved on 29.May.2013 from http://www.fbi.gov/news/stories/2011/june/cyber_062211/cyber_062211
6	On-line news, Retrieved on 29.May.2013 from http://www.fbi.gov/news/stories/2011/november/malware_110911/malware_110911
7	On-line news, Retrieved on 29.May.2013 from http://www.fbi.gov/news/stories/2011/april/botnet_041411
8	On-line news, Retrieved on 29.May.2013 from http://www.fbi.gov/newyork/press-releases/2011/leader-of-armenian-organized-crime-ring-pleads-guilty-in-manhattan-federal-court-to-racketeering

[103] The case concerning Austrian organized crime is retrieved from this website.

9	On-line news, Retrieved on 29.May.2013 from http://www.fbi.gov/newyork/press-releases/2011/manhattan-u.s.-attorney-charges-26-gambino-crime-family-leaders-members-and-associates-on-racketeering-murder-narcotics-firearms-and-other-charges
10	On-line news, Retrieved on 29.May.2013 from http://www.fbi.gov/philadelphia/press-releases/2011/leadership-members-and-associates-of-the-philadelphia-la-cosa-nostra-family-charged-with-racketeering-conspiracy-and-related-crimes
11	On-line news, Retrieved on 29.May.2013 from http://www.fbi.gov/newyork/press-releases/2011/91-leaders-members-and-associates-of-la-cosa-nostra-families-in-four-districts-charged-with-racketeering-and-related-crimes-including-murder-and-extortion
13	On-line news, Retrieved 29.May.2013 from http://www.bi.gov/news/stories/2011/october/gangs_102011/gangs_102011
14	On-line news, Retrieved on 16.Apr.2013 from http://www.fbi.gov/newyork/press-releases/2010/nyfo042010.htm
15	On-line news, Retrieved on 16.Apr.2013 from http://www.fbi.gov/news/stories/2010/october/cyber-banking-fraud/cyber-banking-fraud
16	On-line news, Retrieved on 10.Mar.2013 from http://www.fbi.gov/news/stories/2009/november/atm_111609
17	On-line news, Retrieved on 10.Mar.2013 from http://www.fbi.gov/news/stories/2009/october/phishphry_100709
18	On-line news, Retrieved on 10.Mar.2013 from http://www.fbi.gov/news/stories/2009/june/auctionfraud_063009
19	On-line news, Retrieved on 09.Feb.2013 from http://www.fbi.gov/news/stories/2008/march/innocent_images030608

20	On-line news, Retrieved on 09.Feb.2013 from http://www.fbi.gov/news/stories/2008/october/darkmarket_102008
21	On-line news, Retrieved on 09.Feb.2013 from http://www.fbi.gov/news/stories/2007/june/gambling_060607
22	On-line news, Retrieved on 09.Feb.2013 from http://www.fbi.gov/news/stories/2007/february/iptheft020107
23	On-line news, Retrieved on 26.Jan.2013 from http://www.fbi.gov/news/stories/2006/june/iprny063006
24	On-line news, Retrieved on 26.Jan.2013 from http://www.fbi.gov/news/stories/2006/march/cats030606
25	On-line news, Retrieved on 26.Jan.2013 from http://www.fbi.gov/news/stories/2006/february/innocent_images022406
26	On-line news, Retrieved on 26.Jan.2013 from http://www.fbi.gov/news/stories/2006/april/internet_trends040706
27	On-line news, Retrieved on 26.Jan.2013 from http://www.fbi.gov/news/stories/2004/may/piracy_051704

Table 3: the original sources from China

1	On-line news, Retrieved on 30.June.2013 from http://www.mps.gov.cn/n16/n1252/n1762/n2452/3179808.html
2	On-line news, Retrieved on 30.June.2013 from http://www.mps.gov.cn/n16/n1252/n1762/n2452/3147324.html
3	On-line news, Retrieved on 30.June.2013 from http://www.mps.gov.cn/n16/n1237/n1342/n803715/3296069.htm
4	On-line news, Retrieved on 30.June.2013 from http://www.mps.gov.cn/n16/n1237/n1342/n803715/3330551.html

5	On-line news, Retrieved on 30.June.2013 from http://www.mps.gov.cn/n16/n1237/n1342/n803715/3393152.html
6	On-line news, Retrieved on 30.June.2013 from http://www.mps.gov.cn/n16/n1237/n1342/n803715/3617482.html
7	On-line news, Retrieved on 30.June.2013 from http://www.mps.gov.cn/n16/n1252/n1687/n2227/3414318.html
8	On-line news, Retrieved on 30.June.2013 from http://www.cisaw.cn/html/jishuyuandi/552.html
9	On-line news, Retrieved on 29.May.2013 from http://www.mps.gov.cn/n16/n1252/n1687/n2272/3414264.html
10	On-line news, Retrieved on 16.Apr.2013 from http://www.mps.gov.cn/n16/n1252/n1762/n2452/2634542.html
11	On-line news, Retrieved on 16.Apr.2013 from http://www.mps.gov.cn/n16/n1252/n1762/n2452/2580402.html
12	On-line news, Retrieved on 16.Apr.2013 from http://www.mps.gov.cn/n16/n1252/n1762/n2452/2562633.html
13	On-line news, Retrieved on 16.Apr.2013 from http://www.mps.gov.cn/n16/n1252/n1762/n2452/2461405.html
14	On-line news, Retrieved on 16.Apr.2013 from http://www.mps.gov.cn/n16/n1252/n1762/n2452/2455898.html
15	On-line news, Retrieved on 16.Apr.2013 from http://www.mps.gov.cn/n16/n1252/n1762/n2452/2442526.html
16	On-line news, Retrieved on 16.Apr.2013 from http://www.mps.gov.cn/n16/n1252/n1762/n2452/2442544.html

17	On-line news, Retrieved on 16.Apr.2013 from http://www.mps.gov.cn/n16/n1252/n1762/n2452/2441268.html
18	On-line news, Retrieved on 16.Apr.2013 from http://www.mps.gov.cn/n16/n1252/n1762/n2452/2326791.html
19	On-line news, Retrieved on 10.Mar.2013 from http://www.mps.gov.cn/n16/n1252/n1762/n2452/2260417.html
20	On-line news, Retrieved on 10.Mar.2013 from http://www.mps.gov.cn/n16/n983040/n2040908/n2040938/2043555.html
21	On-line news, Retrieved on 10.Mar.2013 from http://www.mps.gov.cn/n16/n983040/n2040908/n2040938/2043619.html
22	On-line news, Retrieved on 10.Mar.2013 from http://www.mps.gov.cn/n16/n983040/n2040908/n2040938/2043573.html
23	On-line news, Retrieved on 10.Mar.2013 from http://www.mps.gov.cn/n16/n983040/n2040908/n2040938/2043524.html
24	On-line news, Retrieved on 10.Mar.2013 from http://www.mps.gov.cn/n16/n983040/n2040908/n2040938/2043611.html
25	On-line news, on 10.Mar.2013 from http://www.mps.gov.cn/n16/n983040/n2040908/n2040938/2043591.html
26	On-line news, Retrieved on 10.Mar.2013 from http://www.mps.gov.cn/n16/n983040/n2040908/n2040938/2043581.html
27	On-line news, Retrieved on 10.Mar.2013 from http://www.mps.gov.cn/n16/n1252/n1762/1798100.html
28	On-line news, Retrieved on 10.Mar.2013 from http://news.sina.com.cn/w/2009-03-14/112315309043s.shtml

29	On-line news, Retrieved on 10.Mar.2013 from http://news.xinhuanet.com/world/2009-02/25/content_10891681.htm
30	On-line news, Retrieved on 09.Feb.2013 from http://www.mps.gov.cn/n16/n1252/n1762/n2452/137073.html
31	On-line news, Retrieved on 26.Jan.2013 from http://www.mps.gov.cn/n16/n1252/n1762/n2452/128968.html
32	On-line news, Retrieved on 26.Jan.2013 from http://www.mps.gov.cn/n16/n1237/n1342/118206.html
33	Xupan, (24, Aug 2012). The police of Philippine uncovered a fraud gang of China. Global Times, p.03
34	8 terrorists are wanted by the Ministry of Public Security of the People's Republic of China. Yangzhou Times, (22, Oct 2008), p.A10

Table 4: the original sources from Canada

1	On-line news, Retrieved on 30.July.2013 from http://www.rcmp-grc.gc.ca/news-nouvelles/2013/06-27-pangea-eng.htm

Table 5: the original sources from U.K

1	On-line news, Retrieved 30.July.2013 from http://www.soca.gov.uk/news/552-eleven-arrests-as-global-investigation-dismantles-criminal-web-forum
2	On-line news, Retrieved on 30.July.2013 from http://www.soca.gov.uk/news/551-money-laundering-network-jailed-
3	On-line news, Retrieved on 30.July.2013 from http://www.soca.gov.uk/news/543-judge-jails-international-cocaine-trafficker
4	On-line news, Retrieved on 30.July.2013 from

	http://www.soca.gov.uk/news/539-carbon-credit-thieves-jailed
5	On-line news, Retrieved on 30.July.2013 from http://www.soca.gov.uk/news/533-websites-trading-in-stolen-bank-data-targeted
6	On-line news, Retrieved on 30.June.2013 from http://www.soca.gov.uk/news/453-worldwide-arrests-of-on-line-carding-forum-users-
7	On-line news, Retrieved on 30.June.2013 from http://www.soca.gov.uk/news/446-web-domains-seized-in-international-operation-to-target-on-line-fraudsters
8	On-line news, Retrieved on 29.May.2013 from http://www.soca.gov.uk/news/364-smart-phone-malware-highlighted-by-get-safe-on-line-week-
9	On-line news, Retrieved on 16.Apr.2013 from http://www.soca.gov.uk/news/296-meter-cheater-fraud-rips-off-electricity-customers-
10	On-line news, Retrieved on 16.Apr.2013 from http://www.soca.gov.uk/news/292-scareware-alert-to-web-users

Table 6: the original sources from Australia

1	On-line news, Retrieved on 30.July.2013 from http://www.afp.gov.au/media-centre/news/afp/2013/march/federal-and-state-law-enforcement-partnership-dismantles-international
2	On-line news, Retrieved on 30.July.2013 from http://www.afp.gov.au/media-centre/news/afp/2013/march/117kg-of-drugs-seized-in-organised-crime-investigation-spanning-five-countries
3	On-line news, Retrieved on 30.June.2013 from http://www.afp.gov.au/media-centre/news/afp/2012/november/seven-arrested-in-australias-largest-credit-ca

	rd-data-theft-investigation
4	On-line news, Retrieved on 30.June.2013 from http://www.afp.gov.au/media-centre/news/afp/2012/january/Media%20Release%20-%20%20Joint%20agency%20investigation%20dismantles%20organised%20crime%20syndicate
5	On-line news, Retrieved on 30.June.2013 from http://www.afp.gov.au/media-centre/news/afp/2012/september/further-arrests-laid-in-multimillion-dollar-identity-crime-syndicate-investigation
6	On-line news, Retrieved on 29.May.2013 from http://www.afp.gov.au/media-centre/news/afp/2011/november/identity-crime-raids-seize-10000-fake-credit-three-arrested
7	On-line news, Retrieved on 16.Apr.2013 from http://www.afp.gov.au/media-centre/news/afp/2010/november/media-release-operation-smashes-organised-crime-and-counterfeiting-syndicate
8	On-line news, Retrieved on 16.Apr.2013 from http://www.afp.gov.au/media-centre/news/afp/2010/december/warning-on-new-internet-scams
9	On-line news, Retrieved on 10.Mar.2013 from http://www.afp.gov.au/media-centre/news/afp/2009/july/credit-card-manufacturing-equipment-seized-after-raids-on-6-million-syndicate
10	On-line news, Retrieved on 09.Feb.2013 from http://www.afp.gov.au/media-centre/news/afp/2008/May/sydney-man-linked-to-identity-theft-syndicate
11	On-line news, Retrieved on 09.Feb.2013 from http://www.afp.gov.au/media-centre/news/afp/2008/December/22-identified-for-downloading-child-abuse-videos
12	On-line news, Retrieved on 09.Feb.2013 from

	http://www.afp.gov.au/media-centre/news/afp/2007/February/ahtcc-warns-on-internet-employment-scams
13	On-line news, Retrieved on 09.Feb.2013 from http://www.afp.gov.au/media-centre/news/afp/2007/June/afp-integral-in-international-hunt-for-on-line-predators
14	On-line news, Retrieved on 09.Feb.2013 from http://www.afp.gov.au/media-centre/news/afp/2007/December/operation-irenic

Table 7: the original sources from Interpol

1	On-line news, Retrieved on 30.July.2013 from http://www.interpol.int/News-and-media/News-media-releases/2013/N20130619
2	On-line news, Retrieved on 30.July.2013 from http://www.interpol.int/News-and-media/News-media-releases/2013/PR079
3	On-line news, Retrieved on 29.May.2013 from http://www.interpol.int/News-and-media/News-media-releases/2011/N20110117
4	On-line news, Retrieved on 16.Apr.2013 from http://www.interpol.int/Crime-areas/Organized-crime/Asian-Organized-Crime

Before analyzing these cases, three points need to be mentioned: (1) when these cases were reported in the official websites, approximately 100 cases were just categorized according to the nature rather than depicted in detail. Especially in 2010, most of them were collected from the website of the Ministry of Public Security of the People's Republic of China, such as the reports concerning on-line gambling which was organized by criminal groups. (2) Since these cases were retrieved from different official websites, the majority of them were typical and influential at that moment when

they were reported. At the moment when these cases were collected from the websites, they were at different judicial phases: some of them were at the phase when the offenders were wanted by the police, some of them at the phase when the criminals had been arrested, some of them were being prosecuted, and some of them had been given the corresponding verdict. (3) In order to guarantee that these cases are a true reflection of current organized crime during the 10 years, for the sources of these cases, this dissertation refers to the official websites of relative countries' law enforcements agencies, and at least 98% of the cases were obtained from these official websites. Even though these cases were collected from certain official websites, a considerable amount of them involve many countries. These cases can relatively objectively reveal the general situation of present OC in the era of the internet.

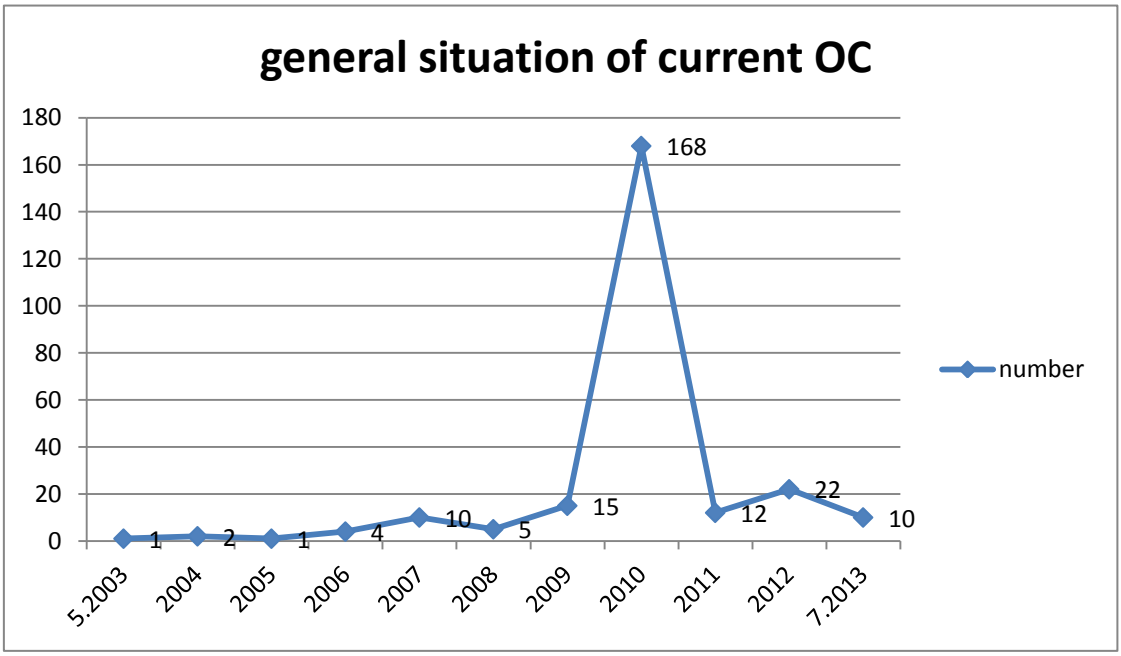
1. General Situation and Trends of Current Organized Crime

In accordance with line chart 1,[104] basically speaking, the general situation of current OC is that the quantity of each year gradually went up from May of 2003 to July of 2013. This chart also illustrates the annual quantity of organized crime: From May of 2003 to 2005, they were one, two and one, in 2006 it rose up to four. The number was 10 in 2007 and 5 in 2008. And then it was 15 in 2009, while the number soared to 168 in 2010. From this point it dropped to 12 in the next year, after 2011 it increased again to 22 in 2012, and then the number went down to 10 during the first half year of 2013.From the May of 2003 to 2006, the annual quantity was different, 2010 saw the peak during the 10 years, from this year it sharply declined to the level of 2009, and then slightly went up to 22 in the next year. Because this dissertation only collects the cases in first half year of 2013, it is unknown whether the annual quantity in 2013 would be more or less than the previous year. The peak that appeared in 2010 can be

[104] The line chart 1 is made by the author of this dissertation.

explained by on-line gambling, which sharply increased, when perpetrated by the organized criminal groups in China.[105] Finally, under the background of globalization and informatization, the general situation of OC in the internet era is revealed by the annual number of these cases, accompanied by the fact that the relationship and connections between different countries are getting much closer, it can be inferred that organized criminal groups are expanding their illegal territory. Not only is the number of pure cyber transnational organized crimes[106] increasing, but also the number of traditional transnational organized crimes which are committed by means of ICTs, either as the channel or the instrument, have been ascending.

Line chart 1: general situation of current OC



2. Penetration of Information Communication Technologies into Current Organized Crime

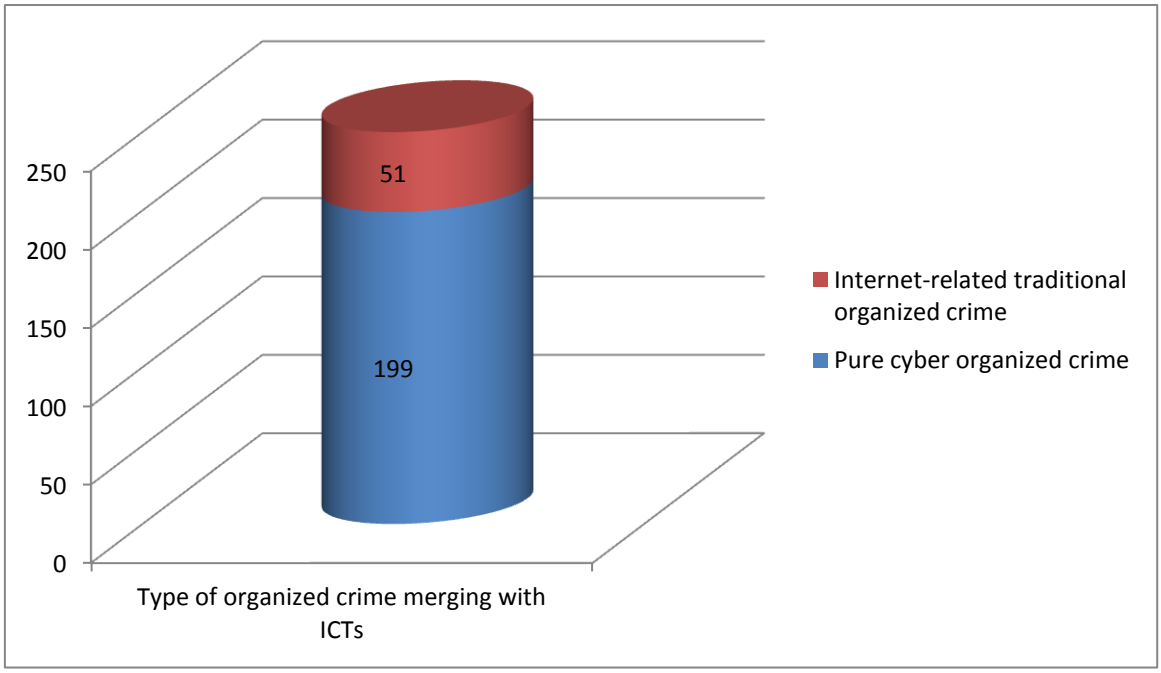
[105] See the bar diagram 7: Trend of on-line gambling.
[106] Pure cyber transnational organized crimes means that organized criminal groups take internet or internet-related devices and software as their criminal objectives.

The bar graph 1[107] depicts two types of OC which are merging with Information Communication Technologies (ICTs). The criterion to distinguish them is whether OCGs use hacker techniques[108]. These two types are the subordinate concept of cyber organized crime (COC). One type is the pure cyber organized crime, which is committed by groups of hackers that carry out organized illegal activities for material profits, power or non-material benefits. In these 250 cases high technology devices and the internet are either tools or targets for committing crime. On-line identity theft and fraud, on-line hacker crime and on-line gambling belong to pure cyber organized crime, since all of these three types used hacker techniques, such as utilizing malware or hacking networks to steal sensitive data, without ICTs, the organized criminal groups cannot commit such on-line crimes. Another type is internet-related traditional organized crime, where for these crimes ICTs are just the tools and channels for committing crimes. In other words, traditional organized crimes have been cyberized by the internet. Taking traditional organized crime as an example, the members of illegal drug trafficking organized groups use the internet and other ICTs to communicate with their accomplices. In accordance with bar graph 1, 199 reported crimes fell within the scope of the former type (pure cyber organized crime), and they accounted for 80%. And 51 reported crimes, accounted for 20%, belonged to the latter type (internet-related traditional organized crime). Combining with line chart 2 and line chart 3,[109] both the figures and annual amount of each type of organized crime reveal that pure cyber organized crime had an obviously substantial increase. Comparatively speaking, as a general tendency the internet related traditional organized crime had also been gradually rising every year. In fact, on the one hand, the infiltration of ICTs into the present organized crime is getting much more serious and complex than in the last century. On the other hand, compared with traditional organized crime, such as murder, robbery,

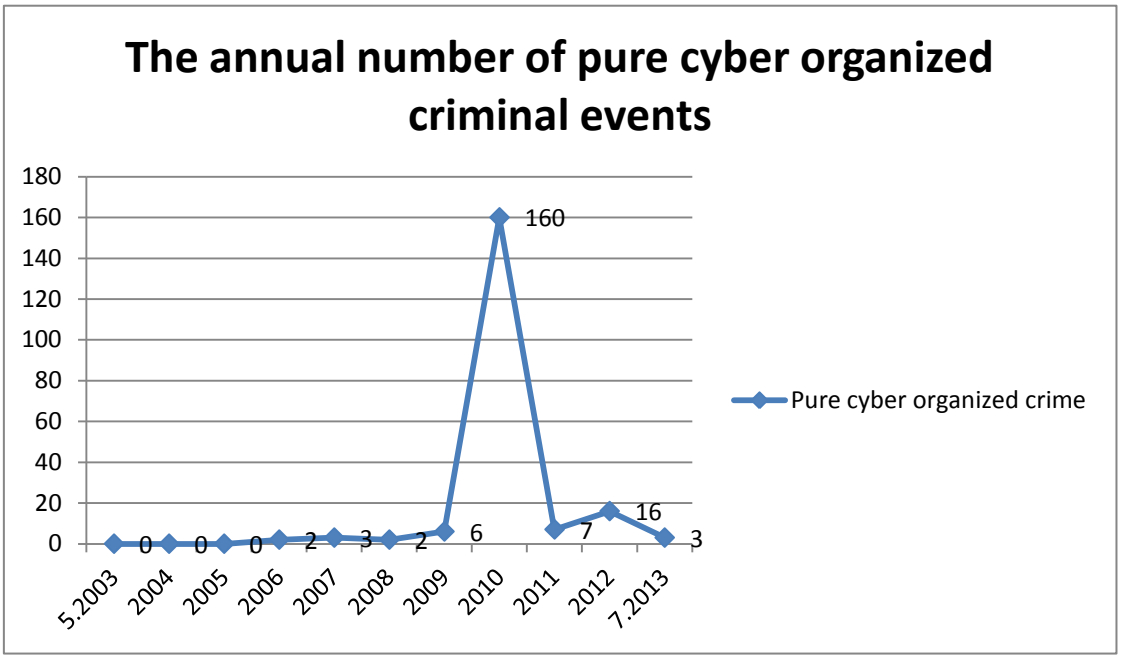
[107] The bar chart 1 is made by the author of this dissertation.
[108] Hacker techniques refer to computer techniques which are used to attacks against computer hardware and software, for example, botnets, malware and network intrusion.
[109] The line chart 2 and line chart 3 are made by the author of this dissertation.

smuggling and trafficking in contraband and pornographic business and so on, pure cyber organized crime accounts for a greater proportion of COC.

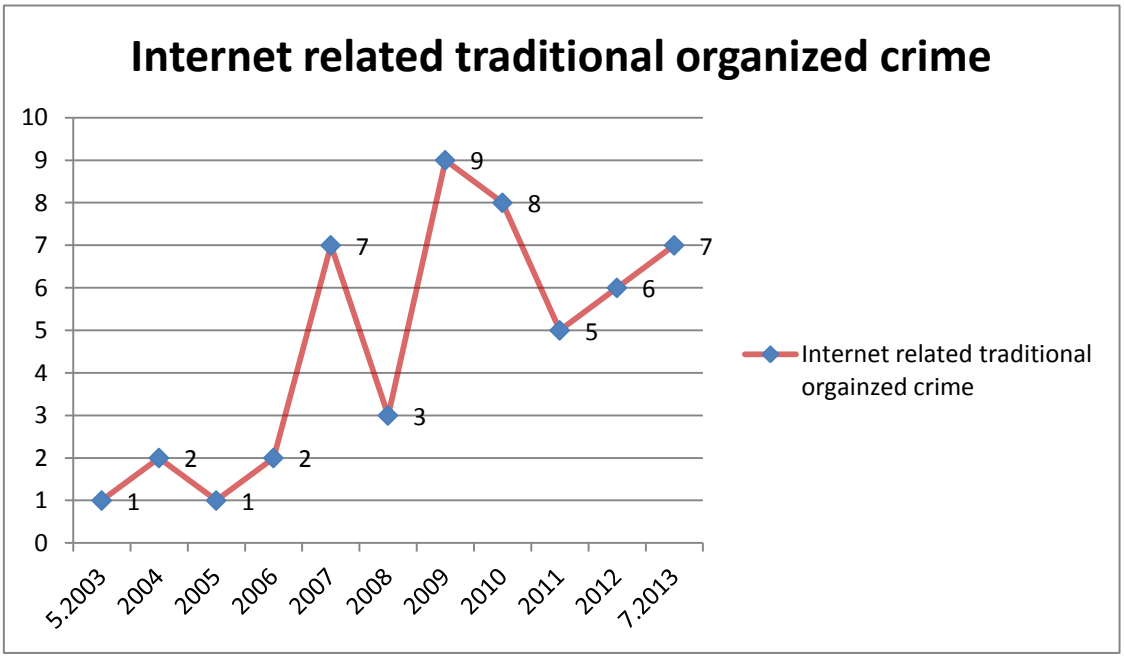
Bar graph 1: types of organized crime merging with ICTs



Line chart 2: annual number of pure cyber organized crime



Line chart 3: annual quantity of internet-related traditional organized crime



3. Analyzing Transnational Characteristics of Current Organized Crime

The focus of this dissertation is CTOC, namely, analyzing the influence of ICTs on the current TOC. Even though not all of these 250 cases fall into the scope of CTOC, analysis of its annual amount and its percentage accounting for cyber organized crime reveals a general increasing trend of current CTOC from May of 2003 to July of 2013. Two categories may be differentiated from each other, respectively, CTOC and domestic cyber organized crime. The criterion of how many countries are involved in it, is is also the main reason why the former type is called "transnational". According to this criterion there are at least two countries involved in CTOC, in contrast, domestic cyber organized crime means only one country is involved. In this dissertation the factors about "involved" which are used to determine whether organized crime is "transnational" are as follows: (a) when one organized crime is committed more than one state is involved; (b) during the process of one organized crime in one state, a substantial part of it, such as preparation, planning, direction or control takes place in another state; (c) one organized crime is committed by an OCG that carries out criminal activities in more than one state; or (d) one organized crime is committed in one state, but it has substantial effects on another state. These four factors have a close relationship with the criteria that are used to determine the jurisdiction of CTOC.[110] One example of CTOC is collected from http://www.soca.gov.uk/[111]: One of the world's largest web forums devoted to trade in stolen credit card data has been disabled by an international law enforcement operation led by the Vietnamese High-Tech Crime Unit (HTCU) and the Criminal Investigation Division (CID) of the Ministry of Public Security of Vietnam (MPSVN), SOCA, the Metropolitan Police Central e-Crime Unit and the FBI. And Simultaneously, CID and HTCU officers in Vietnam arrested eight members of this organised crime group behind the website, and three further arrests of

[110] The corresponding problems of jurisdiction over cyber transnational organized crime will be dealt with in chapter 5.

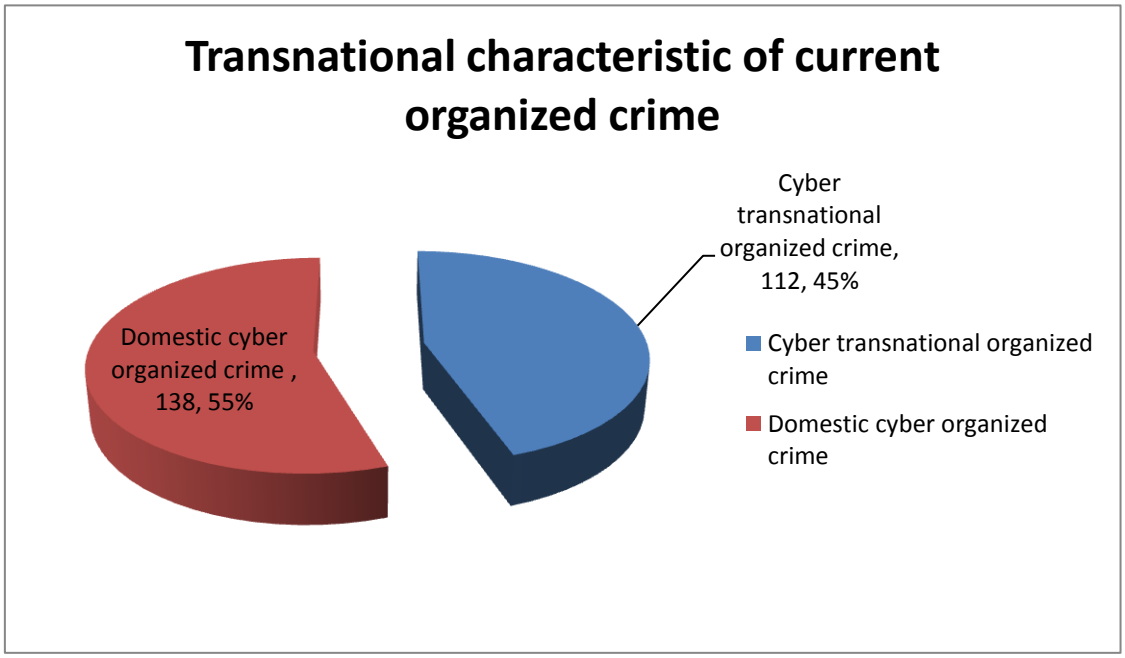
[111] On-line news, retrieved on 29.Auguest.213 from http://www.soca.gov.uk/news/552-eleven-arrests-as-global-investigation-dismantles-criminal-web-forum

significant forum users were made in the UK. The website, which was named as "mattfeuter", had facilitated more than $200m-worth of card fraud worldwide through 'hacking' of commercial entities to harvest and then sell data relating to 1.1 million credit cards. This website had approximately 16,000 members, they could gain access via a secure login and specify the quantity and type of credit card data they wanted, with discounts offered for bulk purchases. The website also had a facility for users to check that card information they were buying was usable. Officers from SOCA, PCeU and the Dedicated Cheque and Plastic Crime Unit (DCPCU) arrested three men in London - a 37 year old from West Ham, a 34 year old from Thornton Heath and a 44 year old from Manor Park. In the US, charges have been brought by the US Department of Justice against Duy Hai Truong, aged 23, of Ho Chi Minh City in Vietnam, one of the suspected ring leaders arrested in Vietnam. Compared with CTOC, domestic cyber organized crime can be explained by the following example[112]: Chinese polices dismantled an organized criminal group which committed internet fraud via a fake website, this website collected and accepted criminal information. The criminals established a website, which IP address is http://www.wangjing110.com, and was named the Chinese internet monitor department. It claimed that it dealt with cyber cases to safeguard consumers' legal rights, and this organized criminal group further posted its website, blog website address and telephone to induce potential victims to contact it. These four factors which determine whether an organized crime is transnational cannot be applied in this case, since China is the only country involved, so this case can be categorized into domestic cyber organized crime. However, both of them are the sub-concepts of cyber organized crime. As pie chart 1 and bar chart 2[113] show: from pie chart 1 the sum of CTOC during the 10 years was 112 and accounted for 45%. And in line with bar chart 2, its annual amounts were one, one, zero, three, three, three, seven, sixty-two, eight, fourteen and 10. In contrast, in accordance with pie chart 1 and bar chart 2, the sum of domestic cyber organized crime cases during the 10 years was 138

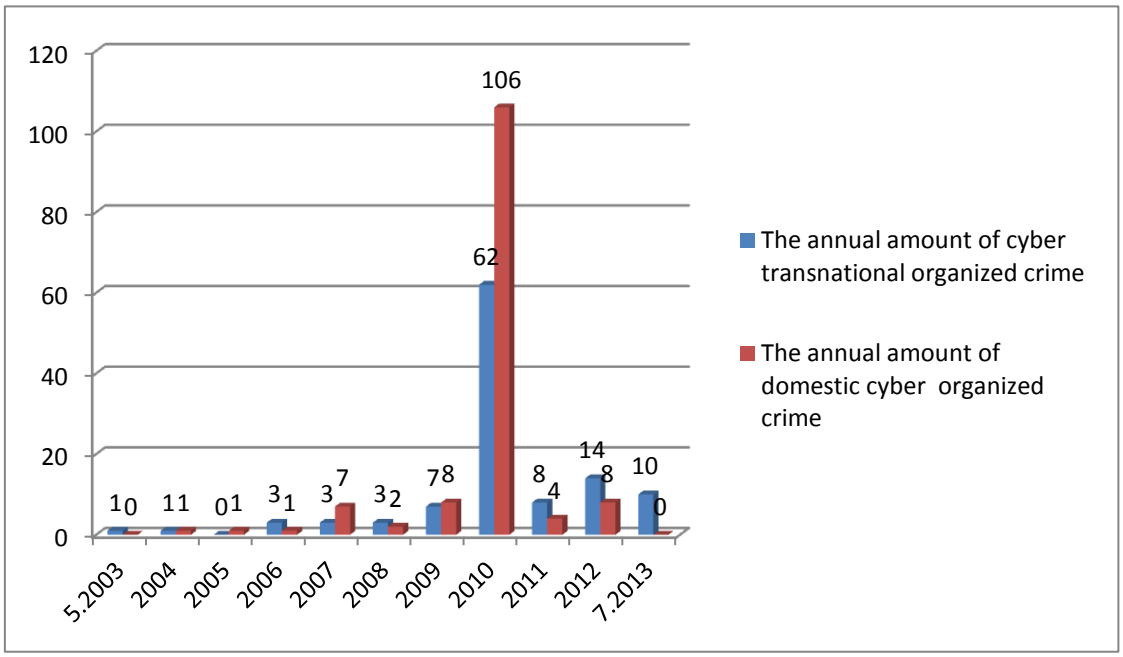
[112] On-line news, retrieved on 29.Auguest.213 from http://www.mps.gov.cn/n16/n1252/n1762/n2452/3179808.html.
[113] Pie chart 1 and bar chart 2 are made by the author of this dissertation.

and accounted for 55% of all cases, and its annual totals were zero, one, one, one, seven, two, eight, one hundred six, four, eight and zero. Obviously, the general trend of current CTOC can be illustrated as: its amounts had been increasing year by year from May 2003 to July 2013 and accounts for almost half of all current cyber organized crimes.

Pie chart 1: Transnational characteristic of current organized crime



Bar chart 2: annual amount of cyber transnational organized crime and domestic cyber organized crime



4. Economic Level of Countries Involved

According to the economic level of the countries which are involved, two categories are included in these 250 cases, respectively, only developed and developing countries are involved. The former refers to the cases that relate only to developed countries, and the latter includes only those cases in developing countries or in developed and developing countries. This criterion assists in analyzing the relationship between different countries' economic level and current cyber organized crime (COC).

On the one hand, cone diagram 1[114] shows the sum of cases (39) that only developed countries are involved in between May 2003 to July 2013, and the sum of cases that

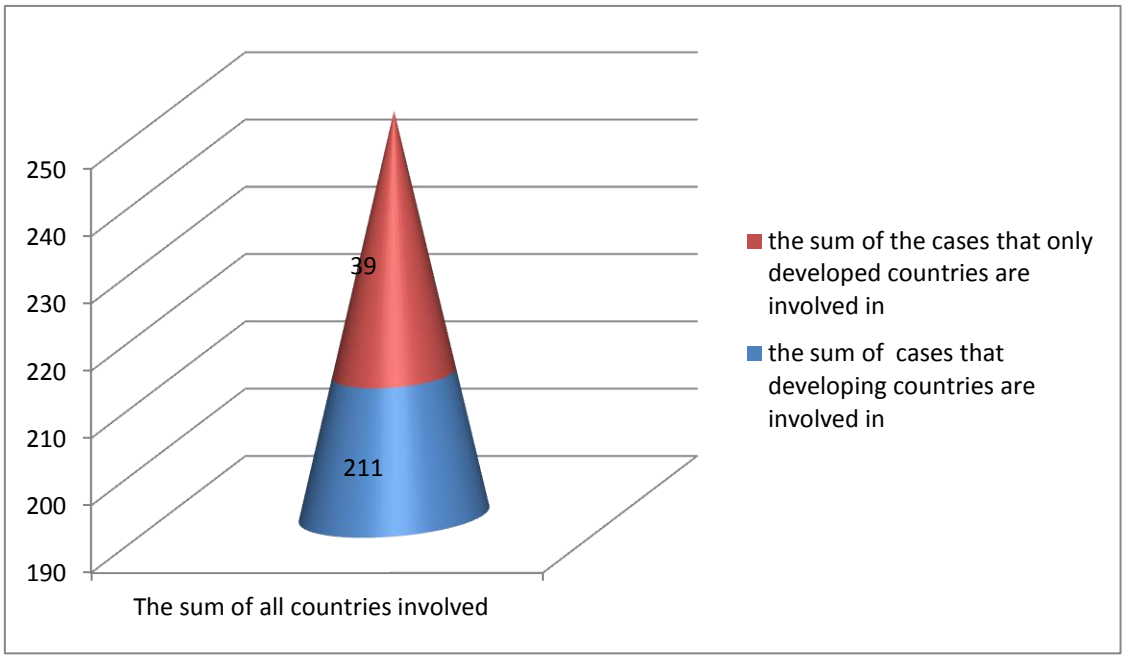
[114] The cone diagram 1 is made by the author of this dissertation.

developing countries were involved in was 211 during the same 10 years. On the other hand, bar diagram 3,[115] draws out the developing trend of current COC in countries of differing economic levels. Among annual cases that developing countries are involved in, the quantity per year grew slowly from May of 2003 to 2009, and the average number was 4 cases. However, in 2010 the sum surged to peak at 161 cases. From that point, the figure rapidly declined to 6 in 2011, and in the next two years, the figure again slowly grew to 11in 2012 and 5 in the first half year of 2013. In contrast, the trend of cases that only developed countries are involved in rose slowly during the 10 years. The figures for each year were zero, one, one, zero, three, three, two, seven, six, eleven and five. As the trend lines in bar diagram 3 show, both of the categories were increasing year after year during the 10 years.

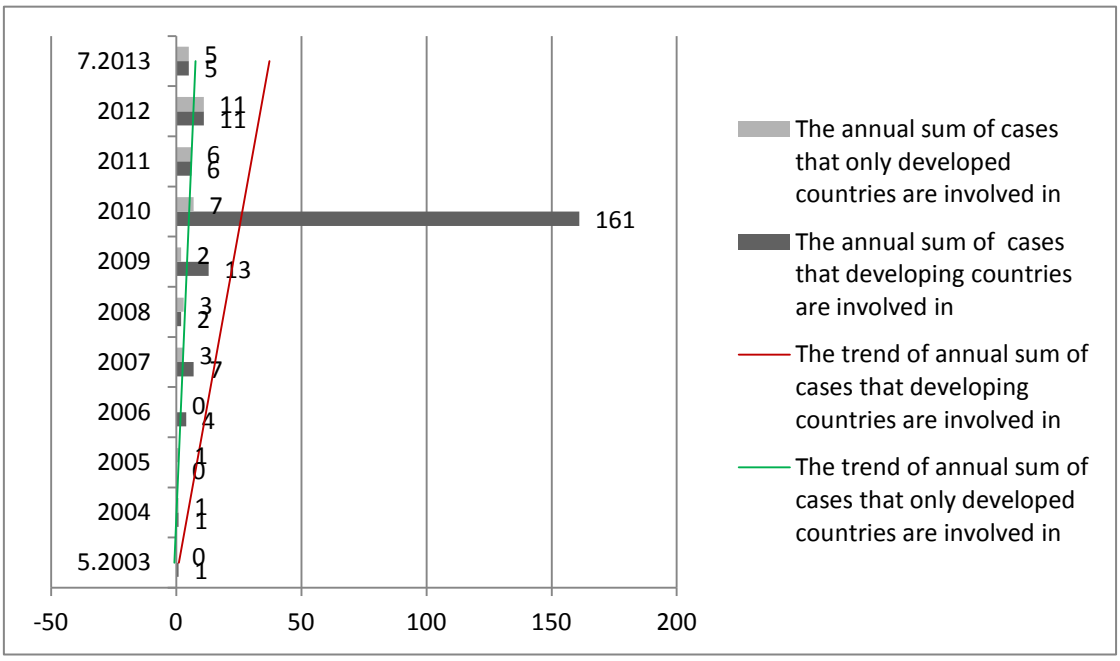
In the light of the above analysis, even though the phenomenon of OC was uncommon in developing countries before the proliferation of the internet, at present the internet and other ICT provide OCGs with chances to cross borders and promote them to develop into CTOC without them existing in other countries. The intervention of the internet into OC results in the link between the economic levels of different countries and OC becoming much weaker.

[115] The bar diagram 3 is made by the author of this dissertation.

Cone diagram 1: sum of involved countries' economic level



Bar diagram 3: annual sum of cases that only developed countries are involved in and that developing countries are involved in



5. Types of Current Cyber Organized Crime

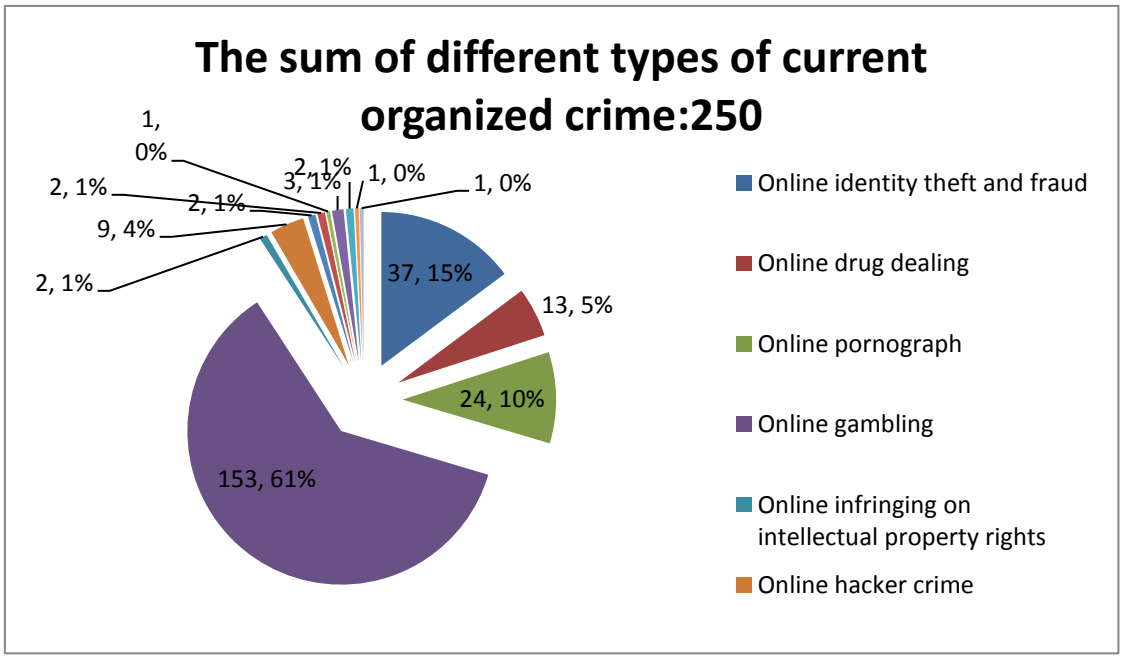
In order to reveal different types of current COC from May 2003 to July 2013, it is necessary to make the statistics of the quantity of each type of cyber organized crime and their percentages during the 10 years, so pie chart 2 is made to illustrate these figures.[116]

By means of analyzing the infringement of legal interests in these 250 cases, pie chart 2 was made to show different types of current COC during the 10 years. In line with pie chart 2, 13 types were categorized, i.e., on-line identity theft and fraud[117], on-line drug dealing, on-line pornography, on-line gambling, on-line infringing on intellectual property rights, on-line hacker crime, on-line selling fake medicine, on-line trafficking in firearms, on-line terrorism, on-line manufacturing and trading counterfeit currency, on-line money laundering, on-line disposal of stolen goods and on-line selling fake invoice. It is obvious that on-line gambling, on-line identity theft and fraud, on-line pornography, on-line drug dealing, on-line hacker crime account for majority of COC, each sum of them are 153, 37, 24, 13 and 9. In contrast, the sum of the other crimes is 14, account for only around 6%.

[116] The pie chart 2 is made by the author of this dissertation.

[117] On-line identity theft and fraud, in this dissertation, include two types of crimes, one is on-line theft, which is committed by cyber organized criminal groups who steal the personal information of individuals or legal entities with hacker techniques or other internet-related skills. The other one is fraud, which is committed by the criminal groups who steal the personal information or the buyers who bought it on-line or offline.

The pie chart 2: Type of current cyber organized crime



One point needs to be emphasized, comparing with on-line identity theft and fraud, on-line drug dealing, on-line pornography, on-line gambling and on-line hacker crime, on-line violating on intellectual property rights, on-line selling fake medicine, on-line trafficking in firearms, on-line terrorism, on-line manufacturing and selling counterfeit currency, on-line money laundering, on-line disposal of stolen goods and on-line selling false bill do not happened so often. Most of the latter types happened in an exact year, which makes statistic has no significant sense to reveal the trends of them.

In accordance with the above analysis, these 250 cases reveal the fact that the OCGs were moving their “battle field” from real physical space to cyber space, and this trend will continue in the future. The statistics indicate that traditional cyber organized crimes were reported much less that the pure CTOC, For example, traditional drug dealing, trafficking in people and smuggling illegal immigrants which related to ICTs were less reported. Pie chart 2 also shows that on-line gambling, on-line identity theft and fraud, on-line pornography, on-line drug trafficking and on-line hacker crime were frequent

COC during the 10years. On the one hand, traditional organized criminal groups started to use ICTs as instruments to commit crimes. On the other hand, new types of COC are booming with the widespread use of the internet.

6. Location characteristics of current organized crime

Bar chart 4 depicts the location characteristics of current organized crime, in other words, in which continent the cases happened. Revealing the location characteristics of current organized crime can supply directions and guidelines when law enforcement agencies combat organized crime, because , by means of knowing this location characteristic the law enforcement agency can focus on addressing major patterns of organized crimes. Before analyzing this characteristic, there is one point which should be noticed, since some cases involve more than one country or one continent, i.e., they are transnational organized crimes, as is showed in bar chart 4, such cases belong to the category of case where more than one continent is involved.

In line with bar chart 4, from May 2003 to July 2013 the cases involving Asia included on-line drug dealing, on-line identity theft and fraud, on-line pornography, on-line gambling, on-line infringing on intellectual property rights, on-line hacker crime, on-line selling fake medicine, on-line weapon trafficking, on-line terrorism, on-line producing and selling counterfeit currency and on-line selling fake invoices, the sum of them were, 2, 16, 15, 151, 1, 15, 1, 2, 1, 1 and 1. Since the sum of on-line identity theft and fraud, on-line pornography, on-line gambling and on-line hacker crimes accounts for 96%[118] among the cases in Asia, it is clear that they are the major patterns of current

[118] The numbers of them are 16, 15, 151 and 15, which are depicted by the bar chart 9.

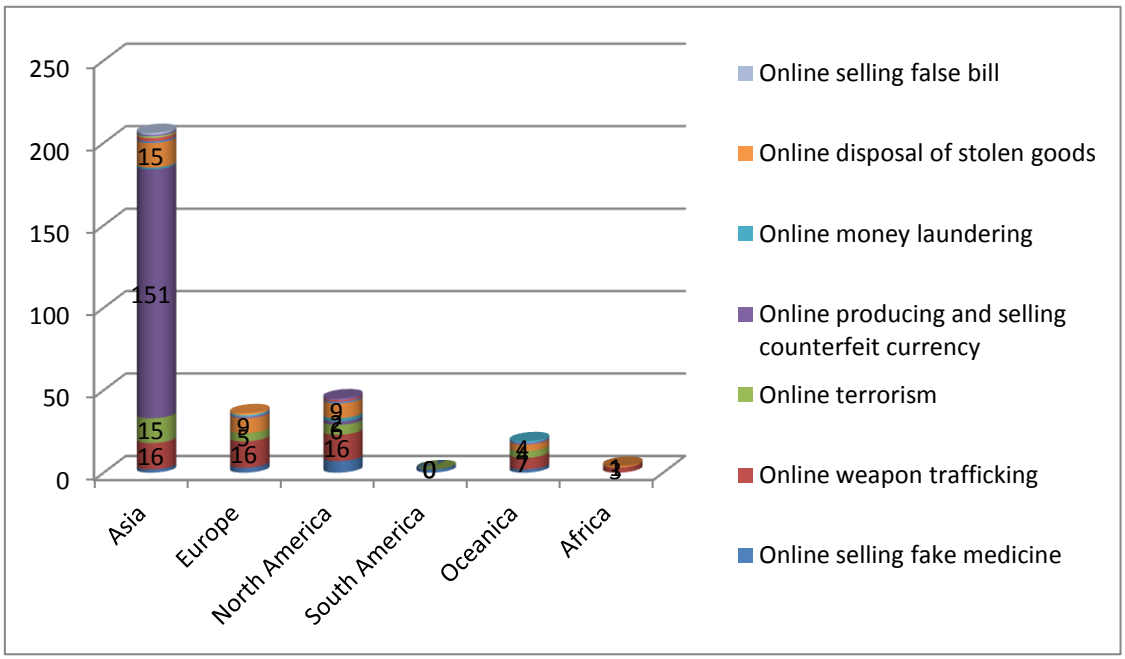
COC in Asia.[119] As for European current illegal cyber activities committed by OCGs, 7 patterns were involved, respectively, on-line drug dealing, on-line identity theft and fraud, on-line pornography, on-line hacker crime, on-line producing and selling counterfeit currency, on-line money laundering and on-line disposal of stolen goods, and the quantities of them were 3, 16, 5, 9, 1, 1 and 1, so on-line identity theft and fraud, on-line pornography and on-line hacker crime were main patterns of COC in Europe.[120] In North America, the major patterns of organized crimes are: on-line drug dealing, on-line identity theft and fraud, on-line pornography, on-line gambling, on-line infringing on intellectual property rights, on-line hacker crime, on-line selling fake medicine, on-line weapon sales and on-line producing and selling counterfeit currency , and the sum totals of them were 7, 16, 6, 2, 2, 9, 1, 1 and 1, so the main patterns in North America were on-line drug dealing, on-line identity theft and fraud, on-line pornography and on-line hacker crime.[121] The cases involving Oceanica included on-line drug dealing, on-line identity theft and fraud, on-line pornography, on-line hacker crime, on-line producing and selling counterfeit currency and on-line money laundering, the number of them were, respectively 2, 7, 4, 4, 1 and 1, so the main pattern of current COC in Oceanica was on-line identity theft and fraud, on-line pornography and on-line hacker crime.[122] In contrast, cases involving South America[123] and Africa[124] were few, the former only had 2 on-line drug dealing cases and the latter had 3 cases of on-line identity theft and fraud and 1 on-line hacker crime.

In the light of analysis of these facts, when looking back at TOC in the pre-internet era, its location characteristics are strongly obvious; for example, drug trafficking and drug dealing usually happened among Southeast Asia, South America and Europe.

[119] The countries involved are China, Japan, South Korea, Thailand, Burma, Cambodia, Philippines, Malaysia, Singapore, Indonesia and India.
[120] The European countries involved include Italy, France, Germany, Austria, Greece, Russia, Spain, Holland, Ukraine, Belarus and Romania.
[121] America, Canada and Mexico are the major countries involved in North America.
[122] In Oceanica Australia is the main country involved .
[123] Columbia is the country involved in South America.
[124] West Africa and Morocco are the main countries involved in Africa.

Comparatively speaking, smuggling immigrants and the illegal pornography business were frequently part of crime patterns across Asia, Africa and Europe. The reasons for the location characteristic of transnational organized crime in the pre-internet era includes the following points: （1） Geographical position, taking drug trafficking and drug dealing as an example, the Andean of South America and Golden Triangle and Afghanistan of Asia are suitable for growing coca and the opium poppy, and these plants are used to produce cocaine and heroin, gradually South America and Asia have developed into the home base of organized criminal groups trafficking and dealing drugs to North America and Europe. (2) Economic level, it can be well explained by trafficking in persons, smuggling immigrants and the illegal pornography business across Asia, Africa and Europe. During the pre-internet age, the majority of Asian and African countries were developing and under-developing countries, people who lived with poor financial conditions wanted to strive for good life in developed areas, like Europe and North America. These factors and conditions provided chances for criminal groups which engaged in trafficking in persons, smuggling immigrants and illegal pornography business across Asia, Africa and Europe. However, compared with past TOC, current OC still has some certain location characteristics, at present the combination of current OC and the internet makes these location features become weaker than in the past, and the reason is as follows: (1) The instantaneity of the internet provides OCGs with great convenience and chances to commit all kinds of crime, so now by means of the internet those OCGs who only engaged in some certain organized crimes in certain area are also seeking new opportunities to fulfil their aims; (2) The borderless nature of the internet means that organized crimes can be conducted in every corner of the world, for example on-line gambling, on-line identity theft and fraud and on-line pornography which, when committed by OCGs, can be carried out worldwide via internet or other ICTs.

Bar chart 4: location characteristic of current organized crime

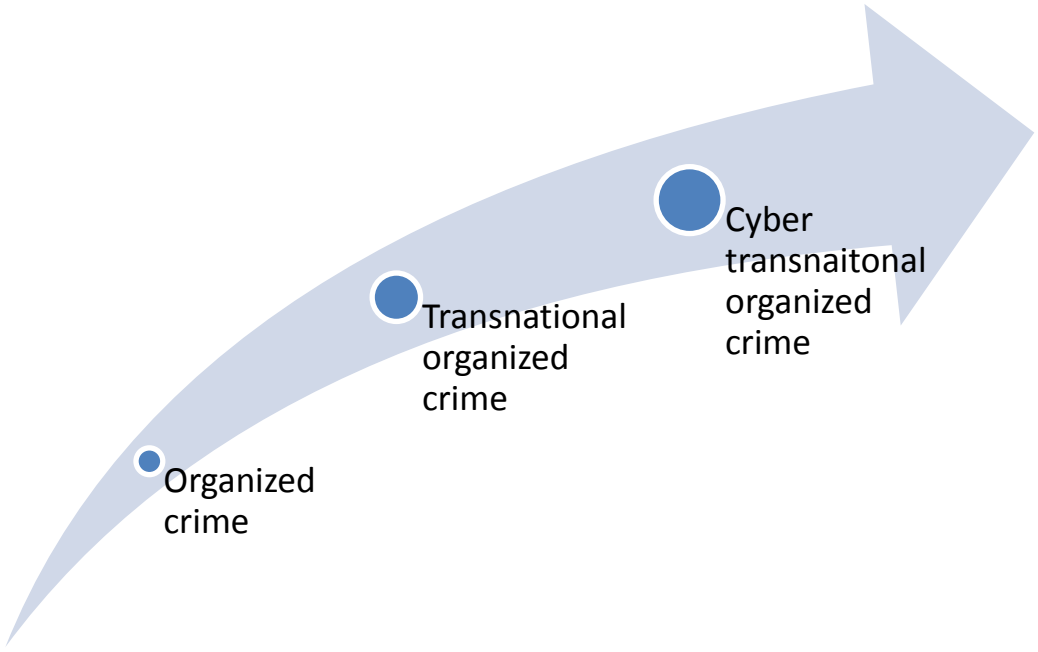


7. Evolving Trend of Transnational Organized Crime

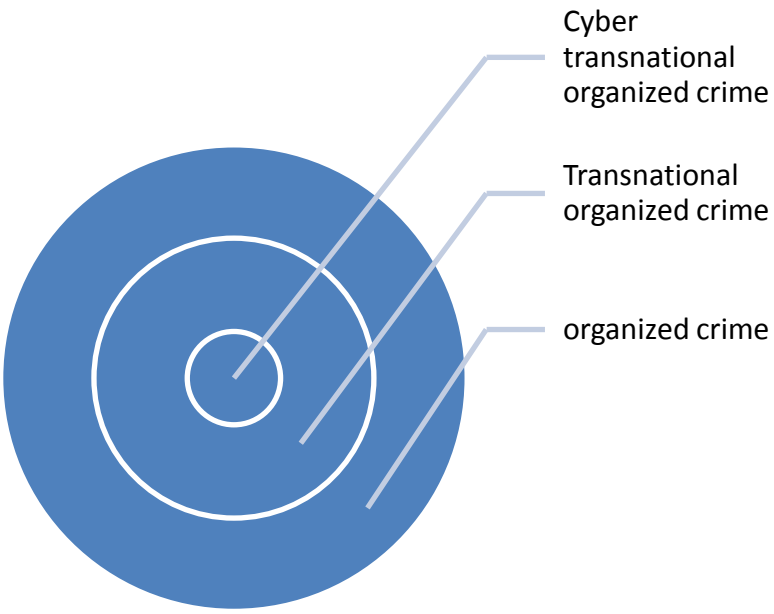
The basis of the aforementioned analysis about current organized crime, flow-process diagram 1 and relationship chart 1 is made[125] to clearly reveal relationships between organized crime, transnational organized crime and cyber transnational organized crime.

Flow-process diagram 1: Evolving phase of organized crime

[125] Flow-process diagram 1 and relationship chart 1 are made by the author of this dissertation.



Relationship chart 1: relationship of different type of organized crime



According to flow-process diagram 1 and relationship chart 1, two points can be concluded: Firstly, cyber transnational organized crime is the highest level of organized crime, and organized crime is at the lowest level among these three types, so that actually, the TOC and CTOC are subordinate concepts of OC; Secondly, there is an

inclusion relationship between organized crime, transnational organized crime and cyber transnational organized crime, which means organized crime can include transnational organized crime and cyber transnational organized crime, and the scope of organized crime is the broadest among these 3 types.

Conclusion

The analysis of these diagrams is made on the basis of 250 cases concerning organized crime in the context of the internet. Since these 250 cases come from certain countries, just based on these 250 cases, some conclusions can be predicated:

- By means of the internet and internet-related ICTs, OCGs start to utilize these high information technologies that can provide more conveniences for their illegal activities. Accordingly, the quantity of TOC and CTOC has been already increasing in these years.

- Connections between organized crime and the internet or ICTs are much closer, accordingly, organized crime can be categorized into two types, one is pure cyber organized crime which cannot be committed without the internet or ICTs; another is internet-related traditional organized crime, so the internet or ICTs are just tools or channels when these crimes are conducted.

- The number of cases of cyber transnational organized crime increased in both of developed and developing countries.

- The scope of illegal activities that organized criminal groups engage in is much broader.

- Location characteristics of cyber transnational organized crime are gradually weakening.

Phases of evolution of organized crime can be described as from organized crime to transnational organized crime to cyber transnational organized crime.

Section 2 New Trends of Organized Crime

The contexts of globalization and advent of ICTs era are interacting with each other. Both of them are major incentive factors that are pushing up the frequency of transnational organized crime. Even though traditional transnational organized crimes have distinct international characteristics, usually they are restricted to some certain areas and territories due to limitations of geographic position, space and time. On the one hand, before the internet age, compared with crimes committed in individual countries, transnational organized crime, confronted by countries or regions, was usually of a few given types, since substantial resources would be needed due to the limitations of geographical position. For instance, traditional transnational organized crimes in China were drug trafficking, drug dealing and illegal smuggling immigrants, while major traditional transnational organized crimes between Europe and its neighbors are trafficking in persons, money laundering, drug trafficking and dealing and piracy. On the other hand, the harm caused by these certain given types of transnational organized crimes was usually restricted to two countries. For example, drug trafficking between China and its Southeast neighbors can illustrate this point well, since these crimes were carried out between China and its neighbors, such as Vietnam. The harm caused by these crimes only affected China and Vietnam. Another side of traditional organized crimes is that they were often carried out in certain districts of one country. For instance, the illegal smuggling immigrants in China often happened in some certain Southeast provinces of China.[126] These 250 cases in section 1 of this chapter reveal one

[126] Yu Zhigang, Li Xiangxia, Case Study concerning Transnational Crime of Chinese Citizens, Journal of National Prosecutors College, Vol. 22 No. 1, Jan. 2014.

fact, that the internet and other ICTs have been pushing forward the development of cyber crime and prompting the integration between cyber crime and organized crime. At present, it can be said that transnational organized crime has evolved into the information phase of transnational organized crime, i.e., cyber transnational organized crime. On the basis of analyzing those 250 cases, two trends can be concluded, one is the informatization of traditional transnational organized crime, and the other is the transnational and organized trend of cyber crimes, i.e., the transformation of cyber crime into organized cyber crime. In the following analysis, these two trends will be discussed in detail.

1. Informatization of Traditional Transnational Organized Crime

The informatization of traditional transnational organized crime can be explained in that the internet and other ICTs are used as instruments, tools or channels of a transnational organized crime. Unlike pure cyber transnational organized crime[127] which can only be committed through the internet and other ICTs. As Robert W. Taylor etc said:[128]

> Using the computer as the instrument of the crime means that the computer is used to gain some other criminal objective. In other words, a burglar uses crowbars and lock picks as the instruments of crime in a fashion similar to the cybercriminal using computer and networks for crimes such as theft, theft service, fraud, and exploitation, and threats or harassment.

Likewise,the internet and other ICTs also can be used as instruments of transnational organized crime. So, the internet and other ICTs provide transnational organized criminal groups with a great number of conveniences.

[127] Pure cyber transnational organized crime refers to high technology devices and the internet being both tools for committing the crime and the target of the crime.
[128] Robert W. Taylor, et al, (2006), *Digital crime and digital terrorism* (p.11), Pearson Education, Inc., Upper Saddle River, New Jersey.

Since the 90s of the last century, organized criminal groups have been increasing and embracing new and advanced technologies to facilitate criminal activity and enhance their criminal operations. Social networking and micro-blogging websites, voice over internet protocol Systems (VoIP systems) and the virtual world enable members of traditional organized criminal groups to communicate globally and discreetly. They are also increasingly employing advanced countermeasures to monitor and target law enforcement while engaging in a host of criminal activity with internet ICTs. The following respects illustrate the informatization of traditional transnational organized crime:

- The internet is used as a communication instruments among members of traditional transnational organized criminal groups. Email, text-chat, real-time voice-based chat, and internet telephone, etc are often used by members of traditional transnational organized criminal groups to communicate with each other. According to the National Gang Threat Assessment 2009 of the United States, gang members typically use the voice and text messaging capabilities of cell phone to conduct drug transactions and pre-arrange meetings with customers.[129] For example, the leader of an African American street gang operating on the north side of Milwaukee used more than 20 cell phones to coordinate the drug-related activities of the gang.[130]

- The internet as a channel for propaganda, intimidation and recruitment. In recent years, transnational organized criminal groups have exploited blogs and popular websites like Youtube and Myspace for propaganda and intimidation. An example was given in the National Gang Threat Assessment 2011 of the United States: the Mexican Drug Trafficking Organizations have posted hundreds of videos depicting

[129] See The National Gang Threat Assessment 2009 of the United States, retrieved on 26. Aug. 2013 from http://www.fbi.gov/stats-services/publications.
[130] Ibid.

interrogations or executions of rival MDTO members.[131] Other postings include video montages of luxury vehicles, weapons, and money set to the music of songs with lyrics that glorify the drug lifestyle. While some of these postings may offer specific recruitment information, they serve more as tools for propaganda and intimidation. Social networking, micro-blogging and video-sharing websites are now more accessible, and versatile, allowing tens of thousands of members of organized criminal groups to easily recruit, receive training and form new alliances nationwide and worldwide.

- Utilizing the internet as the location of transnational organized crimes. This means that transnational organized criminals use the internet to carry out their illegal activities. According to the EU Serious and Organized Crime Threat Assessment 2013, the internet will be an even more important marketplace for illicit commodities and criminal services in the future. Illicit drugs, protected intellectual property, counterfeit goods, firearms, fraudulent identity documents, endangered fauna and flora, counterfeit Euros are all traded over the internet.[132] The internet is also used by transnational organized criminal groups to conduct their illegal business, showcase illegal exploits and facilitate their criminal activity, such as internet drug trafficking and dealing, on-line extortion, internet money laundering and on-line prostitution.

- The internet as a counter-detection instrument. The internet provides OCGs with perceived anonymity and an ability to commit crimes remotely, which makes detection and prosecution by law enforcement agencies more difficult and complex. They are also increasingly employing high level countermeasures to monitor and target law enforcement when carrying out their criminal activities. Members of transnational organized criminal groups are able to exploit a variety of different

[131] See The National Gang Threat Assessment 2011 of the United States, retrieved on 26. Aug. 2013 from http://www.fbi.gov/stats-services/publications..
[132] See The EU Serious and Organized Crime Threat Assessment 2013, retrieved on 26. Aug. 2013 from https://www.europol.europa.eu/latest_publications/31.

tools and techniques to conceal their identity and obscure their offences, such as encrypted messages and password-protected techniques and so on. The criminals are now using the internet to track court proceedings and identify witnesses to avoid the investigation of law enforcement. In addition, the increasing adoption of cloud computing technologies will continue to bring a profound impact to law enforcement investigation. Transnational organized criminal groups would store less data in their computer devices, and the scope of their illegal activities would become much broader, which will probably pose a significant challenge to criminal investigation and digital forensic practice.[133]

2. Transformation of Cyber Crime into Cyber Organized Crime

Except for the informatization of traditional transnational organized crime, another significant tendency which has been revealed by the 250 cases is the transformation of cyber crime into cyber organized crime (COC). In other words, the current transnational organized criminal groups (TOCGs) are increasingly engaging in non-traditional gang-related crimes, or cyber organized criminal groups are starting to commit cyber transnational crimes, which makes cyber crimes evolve into cyber transnational organized crimes. This trend can be depicted as two sides of one coin. Committing non-traditional gang-related crimes via the internet with lower risks, this feature attracts criminal organizations to engage in these types of crimes. It can be well illustrated by white collar crime, such as counterfeiting, identity theft, and mortgage fraud. Primarily they are highly profitable and have much-lower visibility and risk of detection and punishment than drug and weapons trafficking and the other TOC. In the following section, certain types of on-line crime that were committed by TOCGs will be studied to demonstrate this trend.

[133] On-line news, retrieved on 2. Aug. 2014 from http://tech.ccidnet.com/art/1099/20091216/1962171_1.html.

- On-line hacker crime. At the beginning hacker crime was just an uncommon criminal phenomenon. However, with the proliferation of the internet and other ICTs, hacker criminals have realized that hacker technologies are high profitable. Tremendous economic interests attract hackers to work hand in glove with each other. For instance, some cases that have been discussed in the first section were retrieved from the official website of the Ministry of Public Security of the People's Republic of China,[134] the criminals of these cases operated their own illegal hacker businesses in the internet. They programmed all kinds of malicious software, viruses and Trojan horses, and with them they intruded into and controlled public and official computer systems and personal computers. These illegal operations made these computer systems and computers become botnets; they also distributed malicious viruses on the internet and provided hacker technologies and training through the internet. Obviously, these on-line hacker crimes have evolved into COC, and if more than two countries were involved, accordingly, they are CTOC.

- On-line identity theft and fraud. Usually this type has a close relationship with on-line hacker crime, normally on-line identity theft cannot be committed without hacker technologies. Personal identity information, illegally obtained by the offenders of on-line identity theft, is often used to carry out on-line fraud. In other word, if on-line fraud is the target crime, on-line hacker crime and on-line identity theft are instruments of on-line fraud. The cases that were categorized as on-line identity theft and fraud among the 250 cases just tally with this situation. The whole process of these cases are similar, criminals use hacker technology to steal personal identity information and then use the information to commit on-line fraud across many countries, such as China, Korea, Thailand, Burma, Cambodia, the Philippines, Malaysia and Singapore. Much-lower risk and high profitability promote criminals to collude with each other during a period of time to commit these types of crimes, and these crimes gradually develop into cyber transnational organized crime.

[134] On-line news, retrieved on 23.Apr.2014 from http://www.mps.gov.cn/n16/n1252/n1762/n2452/2580402.html.

- On-line gambling. It is a new type of crime with the widespread use of the internet and ICTs. The reason why it distinguishes itself from traditional gambling is that it cannot be committed with the internet and some related software, which illustrates that on-line gambling is a new crime. On the one hand, before the advent of the internet era, gambling was a kind of criminal activity of traditional organized criminal groups, but now with the internet and the other ICTs they start to transfer gambling from the real world into the virtual world. On the other hand, criminals of cyber organized criminal groups are also engaging in on-line gambling. Like the cases which have been mentioned in the first section, criminals have exploited internet ball game gambling programs, rented oversea servers and established many internet ball game gambling platforms. With the convenience of the internet almost all of these illegal activities have become cyber transnational organized crime.

- On-line infringing on intellectual property rights. Before the internet age, on-line infringing on intellectual property rights it was not a traditional organized crime. However, with the widespread use of the internet, a great amount of work has been transferred from traditional form (printed version, sound records, video, etc) into on-line versions with high speed, and the characteristics of traditional copyright, such as being intangible, exclusive, dependent on geography and time, have almost disappeared in the environment of the internet. They gave way to the digitizing public and borderless feature of internet work. These characteristics attract all kinds of criminals cooperating with each other to commit infringements on intellectual property rights on the internet. By means of the internet on-line infringement of intellectual property rights is becoming more organized and easier, and developing into cyber transnational organized crime in the internet era.

In view of the convenience of the internet and the other ICTs, not only do the four aforementioned types of crime reveal the trend of transnational and organized cyber

crimes, but also other crimes that are committed via the internet are appearing and would re-inforce this trend.

3. Conclusion

The aforementioned content of this chapter discussed the interaction and integration of transnational organized crime and cyber crime. Just as the Council of Europe formulated, in its 2004 organized crime situation report, some general hypotheses regarding links between cyber crime and organized crime:[135]

- ICTs offer anonymity, facilitate logistics, and reduce the risks for organized criminals to be prosecuted. They facilitate remotely controlled operations, covert activities, transnational operations, networking, and encrypted communication. [136]

- The penetration and infiltration of banks and corporations along with on-line bank robberies via the Internet are far less risky than burglaries in the real world. Modern computer and communication networks have developed specific characteristics that are useful for criminal perpetrators and difficult for prosecutors to overcome. International computer networks offer anonymity to perpetrators that can be lifted only if all countries crossed by a communication decide to cooperate.[137]

- ICTs are tools for global outreach and search for potential victims.[138]

- ICTs are likely to change the structure of organized crime, that is, the way members organize to carry out crimes (this point will be analyzed in detail in the fourth chapter) .[139]

[135] Allexander Seger, (2012), Cyber Crime and Economic Crime, Maximillian Edelbacher, Peter Kratcoski and Michael Theil (ed), *Financial Crimes: A Threat to Global Security*, CRC Press, p.128-129.

[136] Ibid, p.128.
[137] Ibid, p.128-129.
[138] Ibid, p.129.
[139] Ibid, p.129.

These hypotheses have been proved by the fact of the convergence of transnational organized and cyber crime. However, they are just part of the relationships between these two types of crime. Predictably, these two tendencies, informatization of traditional transnational organized crime and transformation of cyber crime into transnational organized cyber crime, will be more serious and obvious in the future. This has been revealed by the increasing annual number of these two types of crimes and the figures in section 1 of this chapter.

Chapter 3 Investigations into Criminal Legislation and Adjustment of Criminal Policy Combating Cyber Transnational Organized Crime Worldwide in the Internet Age

Just as the news was posted by Interpol on its website, cybercrime has been committed by individuals or small groups of individuals in the past. However, we are now seeing an emerging trend with traditional organized crime syndicates and criminally minded technology professionals working together and pooling their resources and expertise.[140] Even though this problem has attracted the attention of some countries and related international organizations, according to the documents which have been collected by this dissertation, there are no particular domestic legislations and international conventions to control and prevent this new emerging trend, namely the interaction and integration of traditional organized crime and cybercrime. However, it is still necessary to investigate and understand the legislations of some representative countries and, regional and international conventions against organized crime and cyber crime. This work aims to find the absences of existing legislations and conventions against cyber transnational organized crime (CTOC). This chapter focuses on investigating criminal legislation and the adjustment of criminal policy against cyber transnational organized crime in the internet age. As an illegal phenomenon OC came into being much earlier than cybercrime, the interaction and integration of both these crimes can be said to be a new phenomenon. But up to now there has been no domestic law or international convention particular against cyber transnational organized crime. However, there are a great number of existing domestic laws and international conventions against OC and limited quantities of domestic law and regional and international conventions against cyber crime. Of course, the combination and merging of both these types of crimes into each other have attracted the attention of many countries, in the regional and

[140] On-line news (2013), Retrieved on 01. Sept. 2013 from http://www.interpol.int/Crime-areas/Cybercrime/Cybercrime.

international community, for example, the Council of Europe made a forecast about the future of interaction and integration of transnational organized crime and cyber crime in its 2004 organized crime situation report.[141] The work of examining these laws and policies against CTOC will provide a demonstrable basis for the following chapters to analyze loopholes and theoretical problems which have been brought by the evolution of OC and TOC in the era of the internet. Even though this dissertation agrees that the United Nations Convention against Transnational Organized Crime is the most important international legislation combating TOC and the Council of Europe's Convention on Cybercrime is the significant regional legislation against cybercrime, in this chapter, the UNTOC and the Council of Europe's Convention on Cybercrime are not analyzed throughout. The reasons are as follows: (1) this dissertation mainly deals with the absence of these two documents against CTOC, in other words, to prevent the trend of interaction and integration of TOC and cybercrime; (2) From the perspective of this dissertation, the problems brought by the interaction and integration of TOC and cybercrime mainly include three aspects, namely, the absence of particular provisions against CTOC in the UNTOC and the Council of Europe's Convention on Cybercrime (the focus of this chapter), the dilemmas about joint crime theory (the focus of chapter 4) and the conflicts of jurisdictions about CTOC (the focus of chapter 5). So this dissertation only analyzes the provisions related to these three aspects under the UNTOC and the Council of Europe's Convention on Cybercrime; (3) This chapter mainly analyzes the provisions of the UNTOC and the Council of Europe's Convention on Cybercrime that relate to the main topics of this dissertation, namely, the absence of particular provisions against CTOC in UNTOC and the Council of Europe's Convention on Cybercrime, the dilemmas about joint crime theory and the conflicts of jurisdictions about CTOC. There are two reasons as follows: on the one hand, this dissertation agrees with the other provisions of the UNTOC and the Council of Europe's Convention on

[141] Alexander Seger, Cyber Crime and Economic Crime, In Maximillian Edelbacher, Peter Kratcoski and Michael Theil (ed) (2012), *Financial Crimes: A Threat to Global Security*, p.128, CRC Press.

Cybercrime. On the other hand, there is no direct close relationship between the other provisons of these two documents and the main three topics of this dissertation.

Section 1 Investigation into Criminal Legislation against Cyber Transnational Organized Crime Worldwide in the Cyber Age

This section attempts to identify legislations of certain countries against organized crime and cyber crime. The legislations of the USA, member states of the European Union, China, Russia, Japan, regional and international conventions against these crimes are chosen as the representatives.

1. Legislation of the USA

On the one hand, OC in the United States is entirely worldwide, so the legislature of America adopted a quantity of laws or regulations to crack down on OC.[142] On the other hand, in recent years some official websites of America often report news about organized criminal groups using ICTs to commit organized crime.[143] In the aspect of combating cyber crime, since the legislations of every state of America are more or less different from federal legislation, and these state legislations can just be applied in their own territory, in view of this, it is necessary to introduce certain American state and federal legislation against cyber crime.

1.1 Legislation against Organized Crime

[142] Cited in Lu Jianping eds. *Comparative Study of Organized Crime*, Law Press · China, 2004, P.51.
[143] On-line news (2013), Retrieved on 28. Aug.2013 from http://www.fbi.gov/.

As early as the 1970s, the federal government of the United States got through two acts,[144] i,e., the Organized Crime Control Act of 1970[145] and the Racketeer Influenced and Corrupt Organizations Act (RICO),[146] the latter was set as chapter 96 under the title 18 of The United Code. The main clauses of RICO include definitions, prohibited activities, criminal penalties, civil remedies, venue and process, expedition of actions, evidence and civil investigative demands.[147] It stipulated the definition of organized racketeering activities and other procedural regulations, such as evidence and investigations etc. Under RICO, racketeering activity is a type of OC, and RICO provides the definition of racketeer activity as follows:[148]

> "racketeering activity" means (A) any act or threat involving murder, kidnapping, gambling, arson, robbery, bribery, extortion, dealing in obscene matter, or dealing in narcotic or other dangerous drugs, which is chargeable under State law and punishable by imprisonment for more than one year; (B) any act which is indictable under any of the following provisions of title 18, United States Code: Section 201 (relating to bribery), title 18, United States Code: Section 201 (relating to bribery), section 224 (relating to sports bribery), sections 471, 472, and 473 (relating to counterfeiting), section 659 (relating to theft from interstate shipment) if the act indictable under section 659 is felonious, section 664 (relating to embezzlement from pension and welfare funds), sections 891-894 (relating to extortionate credit transactions), section 1084 (relating to the transmission of gambling information), section 1341 (relating to mail fraud), section 1343 (relating to wire fraud), sections 1461-1465 (relating to obscene matter), section 1503 (relating to obstruction of justice), section 1510 (relating to obstruction of criminal investigations), section 1511 (relating to the obstruction of State or local law enforcement), section 1512 (relating to tampering with a witness, victim, or an informant), section 1513 (relating to retaliating against a

[144] They are still effective at present to combat organized crimes
[145] Cited in Lu Jianping eds. *Comparative Study of Organized Crime*, Law Press · China, 2004 ,P.51.
[146] Ibid.
[147] On-line news (2013), Retrieved on 01. Sept.2013 from http://www.law.cornell.edu/uscode/text/18/1961.
[148] On-line resources, retrieved on 6. Aug. 2014 from http://www.organized-crime.de/OCLAWS.htm.

witness, victim, or an informant), section 1951 (relating to interference with commerce, robbery, or extortion), section 1952 (relating to racketeering), section 1953 (relating to interstate transportation of wagering paraphernalia), section 1954 (relating to unlawful welfare fund payments), section 1955 (relating to the prohibition of illegal gambling businesses), section 1956 (relating to the laundering of monetary instruments), section 1957 (relating to engaging in monetary transactions in property derived from specified unlawful activity), sections 2312 and 2313 (relating to interstate transportation of stolen motor vehicles), sections 2314 and 2315 (relating to interstate transportation of stolen property), section 2320 (relating to trafficking in certain motor vehicles or motor vehicle parts), sections 2341- 2346 (relating to trafficking in contraband cigarettes), sections 2421-24 (relating to white slave traffic), (C) any act which is indictable under title 29, United States Code, section 186 (dealing with restrictions on payments and loans to labor organizations) or section 501(c) (relating to embezzlement from union funds), (D) any offense involving fraud connected with a case under title 11, fraud in the sale of securities, or the felonious manufacture, importation, receiving, concealment, buying, selling, or otherwise dealing in narcotic or other dangerous drugs, punishable under any law of the United States, or (E) any act which is indictable under the Currency and Foreign Transactions Reporting Act;

As a particular act targeting OC, RICO has been playing an active role. In order to prevent OCGs from engaging in lawful business, legislatures of America also enacted the Crime Organization Influenced and Corrupt Organizations Act, which defines the categories of criminal activities of OCGs. This act explicitly prohibits OCGs from engaging in four illegal activities, and it also formulates corresponding penalty principles and designs civil remedies to prevent these four criminal activities.[149] Apart from RICO and the Crime Organization Influenced and Corrupt Organizations Act, Witness Security Reform Act of 1984, Sanctions against Organized Crime Ordinance, Organized Crime Law and The Money Laundering Control Act were also adopted to crack down on OC.[150]

[149] Cited in Lu Jianping eds, *Comparative Study of Organized Crime*, Law Press · China, 2004, P.51.
[150] Now these three acts are still used to prevent and control organized crimes

In the aspect of terrorism, on the one hand, at the state level, 15 states had made laws against terrorism by 1986. As for the protected interests under these laws, criminalizing the "possibility of the threat of terrorism" or "the threat of terrorism" as a felony or misdemeanor in different states can be considered as a start that America protects its citizens and its overseas interests. On the other hand, at the federal level there are still special acts, under which judiciary regulations were stipulated against international terrorism outside the boundary of America. For example, the Crime Control Act of 1984[151] was adopted by the Congress of America, and the item of 1203 of its eighteenth chapter is the clause concerning the hostage issue. The Omnibus Diplomatic Security and Anti-terrorism Act of 1986[152] was also adopted by the Congress, and item 2331 within its chapter 18 is described as: the federal government of the USA holds jurisdiction over overseas murders, a great number of deaths caused by negligence, violence and conspiracy as long as these crimes targeted citizens of the USA or its national interests.[153]

Apart from the above legislations, America was active in respect of Anti money-laundering. In criminal theory, money-laundering is usually regarded as downstream crime of OC. The Currency and Foreign Transactions Reporting Act of 1970 and the Bank Secrecy Act of 1970 were adopted for anti-money laundering, but both of the two acts just oblige banks to shoulder the duty to report to control money laundering rather than criminalize money laundering activities. In 1986, money laundering was criminalized by the Money Laundering Control Act of 1986. And in the following years, America continuously adopted a series of acts to control money laundering. For example, the Money Laundering Protection Improvements Act of 1988,

[151] Cited in Lu Jianping eds, *Comparative Study of Organized Crime*, Law Press · China, 2004, P.52.
[152] Ibid.
[153] These Acts at state and federal level are still effective.

Financial Institutions Reform, Recovery and Enforcement Act of 1989, Crime Control Act of 1990 and Annunzio-Wylie Anti-Money Laundering Act of 1992. In 1987 the Federal Sentencing Guidelines were enacted, and some particular chapters of these guidelines set a criminal penalty for money-laundering. Item 1956 of the Money Laundering Control Act of 1986 provided for doers who knowingly and willfully transport or transfer financial capital from illegal activities. On the contrary, item 1957 of this Act concerns the transaction of non-financial property which comes from some certain illegal activities. Furthermore, in 1994 America adopted the Money Laundering Suppression Act, which improved the requirements of money-laundering in cash transaction reports and emphasized anti-money laundering via non-banking financial institutions. In order to sharply strike money laundering, a customer identity check system and a suspicious transaction reporting system were also set up by the USA.[154]

1.2 Legislation against Cyber Crime

In this part the substantive criminal laws and legislations of America against cyber crime will be introduced at state and federal level.

1.2.1 Substantive Criminal Law at State Level

[154] These Acts since the 1970s reveal the development of American legislations anti-money laundering, and they still have binding force when combating money laundering.

At the level of state, almost all states have particular statutes to combat cyber crimes. In summary, the content of related laws against cyber crime can be categorized into 11 aspects.[155]

- Expanding the scope of the traditional definition of property on the basis of existing laws, and criminalizing cyber crime as traditional crime. For example, by identifying electronic information and computer techniques as property, in the case of stealing such property, offenders can be convicted of larceny.

- A great number of states criminalize tampering, damaging, deleting or destroying computer programs or files as sabotage.

- All state laws regard any accessing to or utilizing another's computer program without authorization as deliberate trespassing.

- A majority of state laws stipulate that activity which obstructs the legal user from operating the systematic functions of their computer, should be considered as a crime.

- Numerous state laws criminalize the transmission of a computer virus, such as embedding and transmitting a computer virus through telephone wire or computer disk, as illegal insertion.

- Some of state laws categorize the activities of deliberate trespassing in a computer system and tampering with or deleting computer data or illegally reproducing a computer program or data as crimes of infringing on intellectual property rights. Some state laws criminalize the aforementioned types of activities as crimes, even though they do not cause serious consequences. And some other states laws even require that the aforementioned activities must be committed with the aim of profit-making or causing economic loss to victims.

[155] Liu Xiaoli and Zhang Liyun, Overview of U.S. Computer Crime Legislation, *Network Security Technology and Application*, Issue 8 (2007).

- Criminalizing aiding or abetting conduct. Some state laws consider aiding or abetting people to commit other crimes via a computer, as crimes.
- Some states criminalize the conduct of illegally possessing a computer system or its contents as illegal possession.
- Online invasion of privacy. Some state laws stipulate that as long as offenders trespass in computer system and examine its contents, this act constitutes online invasion of privacy.
- Unaccomplished offense or conspiracy. Some state laws identify unaccomplished offense or conspiracy to commit cyber crimes as crimes, even equating them with an offense which has been committed.
- Some state laws stipulate that there is a duty to report cyber crime to law enforcement agencies in time, otherwise, breaching it will be considered as crime.

1.2.2 Substantive Criminal Law at Federal Level

At the level of federal law, the first particular federal law against cyber crime, Counterfeit Access Devices and Computer Fraud and Abuse Act, was adopted in 1984, and was further amended in 1986, 1989, 1990, 1994 and 1996.[156] On the one hand, these amendments broaden the application and scope of this act. On the other hand, they further clarify and define some terminologies, and finally this act developed into the Computer Misuse Act Amendments. 7 illegal activities constitute cyber crime under Computer Misuse Act Amendments:

Whoever: [157]

[156] It is still effective at present
[157] On-line resources, retrieved on 07.Aug.2014 from http://www.cybercrimelaw.net/US.html.

(1) having knowingly accessed a computer without authorization or exceeding authorized access, and by means of such conduct having obtained information that has been determined by the United States Government pursuant to an Executive order or statute to require protection against unauthorized disclosure for reasons of national defense or foreign relations, or any restricted data, as defined in paragraph y of section 11 of the Atomic Energy Act of 1954, with reason to believe that such information so obtained could be used to the injury of the United States, or to the advantage of any foreign nation willfully communicates, delivers, transmits, or causes to be communicated, delivered, or transmitted, or attempts to communicate, deliver, transmit or cause to be communicated, delivered, or transmitted the same to any person not entitled to receive it, or willfully retains the same and fails to deliver it to the officer or employee of the United States entitled to receive it;

(2) intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains-

(A) information contained in a financial record of a financial institution, or of a card issuer as defined in section 1602 (n) of title 15, or contained in a file of a consumer reporting agency on a consumer, as such terms are defined in the Fair Credit Reporting Act (15 U.S.C. 1681 et seq.);

(B) information from any department or agency of the United States; or

(C) information from any protected computer if the conduct involved an interstate or foreign communication;

(3) intentionally, without authorization to access any nonpublic computer of a department or agency of the United States, accesses such a computer of that department or agency that is exclusively for the use of the Government of the United States or, in the case of a computer not exclusively for such use, is used by or for the Government of the United States and such conduct affects that use by or for the Government of the United States;

(4) knowingly and with the intent to defraud, accesses a protected computer without authorization, or exceeds authorized access, and by means of such conduct furthers the

intended fraud and obtains anything of value, unless the object of the fraud and the thing obtained consists only of the use of the computer and the value of such use is not more than $ 5.000 in any one-year period;

(5) (i) knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer;

(ii) intentionally accesses a protected computer without authorization, and as a result of such conduct recklessly causes damage; or

(iii) intentionally accesses a protected computer without authorization, and as a result of such conduct, causes damage; and

(B) by conduct described in clause (i), (ii), or (iii) of subparagraph (A), caused (or, in the case of an attempted offense, would, if completed, have caused

(i) loss to 1 or more persons during any 1-year period (and, for purposes of an investigation, prosecution, or other proceeding brought by the United States only, loss resulting from a related course of conduct affecting 1 or more other protected computers) aggregating at least USD 5,000 in value;

(ii) the modification or impairment, or potential modification or impairment, of the medical examination, diagnosis, treatment, or care of 1 or more individuals;

(iii) physical injury to any person;

(iv) a threat to public health or safety; or

(v) damage affecting a computer system used by or for a government entity in furtherance of the administration of justice, national defence, or national security;

(6) knowingly and with intent to defraud traffics (as defined in section 1029) in any password or similar information through which a computer may be accessed without authorization, if

(A) such trafficking affects interstate or foreign commerce; or

(B) such computer is used by or for the Government of the United States;

(7) with intent to extort from any person any money or other thing of value, transmits in interstate or foreign commerce any communication containing any threat to cause

damage to a protected computer; shall be punished as provided in subsection (c) of this section.

As far as the penalty of the aforementioned crimes is concerned, according to this amendment, the offenders can be sentenced to a term of imprisonment of no less than 1 year or fined, or at the most a term of imprisonment of less than 20 years or fined. The penalty for an unaccomplished offense is the same as for an accomplished offense. Apart from this special legislation against cyber crime, there are still dozens of federal laws or acts [158] to accuse cyber crime offenders, such as the copyright act, telecommunication privacy act, mail and telegram fraud act and child pornography prevention act, etc. In 2003, the president of America, Bush signed an act Controlling the Assault of Non-solicited Pornography Marketing to anti-spam.[159]

These aforementioned legislations of the USA combating OC and cyber crimes are still valid at present. In the aspect of legislations against OC, since they were enacted before the proliferation of the internet, cyber crimes were not included in the scope of OC, which is revealed by the definition of racketeering activity under the Racketeer Influenced and Corrupt Organizations Act. Under this definition only mail fraud and wire fraud were included in the scope of racketeering activity related to OC. In respect of legislations against cyber crimes, only the illegal activities of targeting a computer, computer data or computer systems were criminalized, but the other crimes which are committed via a computer, internet or internet-related ICTs were not included., So crimes where the internet or internet-related ICTs are instruments and channels for a single offender or OCGs, are excluded from cybercrime. The weaknesses of legislation about OC and Cybercrime make them less powerful when combating cyber organized crimes, even cyber transnational organized crimes.

[158] These acts are still effective.
[159] Liu Xiaoli and Zhang Liyun, Overview of U.S. Computer Crime Legislation, *Network Security Technology and Application*, Issue 8 (2007).

2. Legislation of the European Union

Europe is one of the cradles of organized crime, so the European Union and almost all its member states have legislations against organized crimes and cyber crimes.[160] The following text briefly introduces some typical countries' legislations against both of these crimes.

2.1 Legislation of Italy

Legislation against organized crime and cyber crimes in Italy can be respectively introduced as follows:

2.1.1 Legislation against Organized Crime

The generation and rampancy of OC in Italy have been impelling authorities of Italy to enact legislation against OC. Apart from provisions related to OC under the criminal code of Italia, a series of statutes were also adopted to combat OC. For example, the fifteenth statute of 1980 and the 304th statute of 1982[161] are also against OC. According to these two statutes, as long as crimes meet the criteria set by the following items, they should be considered as organized crime: A. the first article of the 15th statute of 1980 stipulates that the aim of crime is to carry out terrorism or overthrow constitutional

[160] Lu Jianping eds, *Comparative Study of Organized Crime*, Law Press · China, 2004, P.51.
[161] These two statutes are still effective in Italy

order; B. utilizing terrorist violence that links with a Mafia syndicate, terrorist violence which under the servitude or intimidatory violence that are the result of keeping the secretive rules of criminal groups (the item c of 416th article of criminal code), or assisting a mafia syndicate to make their illegal activities to be committed more easily (the 8th article of 203th statute of 1991).[162] Some other special crimes are also included in the scope of OC, such as money laundering, drug trafficking and drug manufacturing offenses. In order to effectively control OC, both criminal procedure law and prison law also are used to combat this type of crime. In the aspect of criminal procedure law, it stipulates temporary powers of detention and shortens the time period for investigation. In 1992 Italy adopted a special ordinance[163] to crack down on the Mafia, its article 306 states: once a member of mafia is brought to trail, if he could not explain the source of his/her money, articles and assets, or property which is out of proportion with his/her lawfully earned income, all of these aforementioned articles should be seized.[164] In 1991 the Mafia Repentance Law[165] was adopted, which provides that, the penitent who breaks away from the mafia and his/her relatives can be entitled to life-long welfare supplied by the government, and remission of punishment for the crimes which were committed by him/her in the past.[166] In the respect of legislations against money laundering, there were a series of ordinances between 1978 and 1993.[167] Article 3 of statute of 21.3.1978 supplemented item 2 under the article 648 of the Criminal Code, which provides that the predicated offence of money laundering includes armed robbery, extortion and the crime of hostage taking, but drug crime is excluded. Until 1990, as the signatory of the UN Drug Conventions, in order to implement the duty of this convention, Italy promulgated the 55th ordinance to classify drug crime as the predicated offence of money laundering. On 08.06 of 1992, Italy issued its 306th ordinance. It provides that anyone who is being investigated due to serious crime, if he possessed

[162] Francesc. Balazuo. Italian Legislation on Organized Crime. *Juvenile Deliquency Research*. Issue 5-6 (1997).
[163] It still has binding force
[164] Lu Jianping eds, *Comparative Study of Organized Crime*, Law Press · China, 2004, P.51.
[165] This ordinance is still effective at present.
[166] Lu Jianping eds, *Comparative Study of Organized Crime*, Law Press · China, 2004, P.51.
[167] They are still effective.

properties that are out of proportion with his legal income and could not explain the legal sources of this property, he should be sentenced to a fixed-term imprisonment of one year to four years along with being punished by confiscation of property. Furthermore, since Italy signed and approved the European Council's Money Laundering Conventions of 1990, it promulgated the 328th ordinance on 09.08 of 1993.[168] It amplified the offence of money laundering to all types of serious crime, which further supplements the 648th ordinance of the criminal code.[169]

2.1.2 Legislation against Cyber Crime

The Senate of the Italian Parliament on February 27 (2008) approved and ratified the Convention on Cybercrime. The provisions against cyber crime in the criminal code of Italy are as following: [170]

> Penal Code Article 615 ter: Unauthorized access into a computer or telecommunication systems: Anyone who enters unauthorized into a computer or telecommunication system protected by security measures, or remains in it against the expressed or implied will of the one who has the right to exclude him, shall be sentenced to imprisonment not exceeding three years.
>
> The imprisonment is from one until five years:
>
> 1) if the crime is committed by a public official or by an officer of a public service, through abuse of power or through violation of the duties concerning the function or the service, or by a person who practices - even without a licence - the profession of a private investigator, or with abuse of the capacity of a system operator.
>
> 2) if to commit the crime the culprit uses violence upon things or people, or if he is manifestly armed.

[168] The 55th ordinance, 306th ordinance and 328th ordinance are still effective in Italy.
[169] Ibid.
[170] On-line resources, retrieved on 08. Aug. 2014 from http://www.cybercrimelaw.net/Italy.html.

3) if the deed causes the destruction or the damage of the system or the partial or total interruption of its working, or rather the destruction or damage of the data, the information or the programs contained in it.

Should the deeds of the 1st and 2nd paragraphs concern computer or telecommunication systems of military interest or (concerning) public order or public security or civil defence or whatsoever public interest, the penalty is - respectively- one to five years or three to eight years' imprisonment. In the case provided for in the 1st paragraph, the crime is liable to punishment only after an action by the plaintiff; the other cases are prosecuted "ex-officio".

-615 quater: Illegal Possession and Diffusion of Access Codes to Computer or Telecommunication Systems: Whoever, in order to obtain a profit for himself or for another or to cause damage to others, illegally gets hold of, reproduces, propagates, transmits or deliver codes, key-words or other means for the access to a computer or telecommunication system protected by safety measures, or however provides information or instructions fit to the above purpose, is punished with the imprisonment not exceeding one year and a fine not exceeding 10 million liras.

The penalty is imprisonment from one until two years and a fine from 10 until 20 million liras in the case of one of the circumstances numbered in 1 and 2 in the 4th paragraph of article 617-quater.

-615 quinquies: Diffusion of Programs Aimed to Damage or to Interrupt a Computer System: Whoever propagates, transmits or delivers a computer program - edited by himself or by another - with the aim and the effect to damage a computer or telecommunication system, the data or the programs contained or pertinent to it, or rather the partial or total interruption or an alteration in its working, is punished with imprisonment not exceeding two years and fined not exceeding 20 million liras.

2.2 Legislation of Germany

Germany also does not have a particular law to counter cyber transnational organized crime, so, in order to check how COC or even CTOC are combated or prevented, the legislation of Germany will be introduced in respect of organized crime and cyber crime.

2.2.1 Legislation against Organized Crime

German legislation against OC will be introduced from the aspects of criminal law, criminal procedure law and particularly criminal law. Firstly, the conduct of establishing OCGs is criminalized under article 129 of the German Criminal Code. Secondly, provisions that strengthen the protection of witness and undercover scouts were added to article 68 and article 110 of the criminal procedure law. Apart from these, in 1992 the legislature promulgated the Prevention and Control of Drug Trafficking and Other Forms of Organized Crime Act, which is also named Organized Crime Act.[171] It systematically establishes each accusation about OC, principles of culpability and criminal justice measures. In the respect of legislation for combating terrorism, on 19.12 of 1982, the Former Federal Republic of Germany promulgated the Act of Punishing Terrorist Activities. In order to counter the downstream crime of OC, money laundering, the Prevention and Control of Drug Trafficking and Other Forms of Organized Crime Act of 1992 clearly defines money laundering as a crime, which adds a new accusation under article 261 of the criminal code. In order to implement the EU Anti-Money Laundering Directives, in 1993 the Anti-Money Laundering Act was put into effect on 29.11, which established the legal responsibility of financial systems to control money laundering. Furthermore, the Act of Improving against Organized Crime was adopted in 1998, which broadens the scope of the offence of money laundering and enhances its

[171] It is still effective at present.

punishment.[172] At the international level, Germany joined in the UN drug conventions in1993.[173]

2.2.2 Legislation against Cyber Crime

On 20.September.2006 the government of Germany proposed a new draft law on cybercrime aiming to close any remaining loopholes. Germany promulgated the 41st amendment of the Criminal Code, which is also the implementation of the Convention on Cybercrime of Europe of 23.21.2001 and EU Council Framework Decision 2005/222/JHA [174] on Attacks against Information Systems of 24.2.2005.This amendment effective for the suppression of the increasingly serious cyber organized crime in Germany.[175] Before this amendment, there were two kinds of cybercrimes that were divided into four accusations under German criminal code; they were respectively, invasion of computer data and security of information system (prying into data under the article 202a, modifying data under the article of 303a, and destroying a computer under 303b) and cyber crime by means of computer or internet (internet fraud under the article 263a).[176] After this amendment, the Current Penal Code is as follows[177]:

Section 202a. Data Espionage:

(1) Any person who obtains without authorization, for himself or for another, data which are not meant for him and which are specially protected against unauthorized access, shall be liable to imprisonment for a term not exceeding three years or to a fine .

---

[172] The Anti-Money Laundering Act and the Act of Improving against Organized Crime are still effective under the present situation.

[173] Lu Jianping eds, *Comparative Study of Organized Crime*, Law Press · China, 2004, P.53.

[174] EU Council Framework Decision 2005/222/JHA has been replaced by the Directive 2013/40/EU the European Parliament and of the Council of 12 August 2013 on attacks against information systems.

[175] Ulrich. Sieber, *The Threat of Cybercrime in Organized Crime in Europe: The Threat of Cybercrime Situation Report 204*, Council of Europe Publishing 2005, p.81-218.

[176] Pi Yong, The German Cyber Crime Legislation under the Background of Integration of European Criminal Law. Peking University Law Journal, Vol.23，No.5 (2011), p. 1038-1060.

[177] On-line resources, retrieved on 09.Aug.2014 from http://www.cybercrimelaw.net/Germany.html.

(2) Data within the meaning of subsection 1 are only such as are stored or transmitted electronically or magnetically or in any form not directly visible.

Section 303a. Alteration of Data

(1) Any person who unlawfully erases, suppresses, renders useless, or alters data (section 202a(2)) shall be liable to imprisonment for a term not exceeding two years or to a fine.

(2) The attempt shall be punishable.

Section 303b. Computer Sabotage

(1) Imprisonment not exceeding five years or a fine shall be imposed on any person who interferes with data processing which is of essential importance to another business, another's enterprise or an administrative authority by:

1. committing an offense under section 300a(1) or

2. destroying, damaging, rendering useless, removing, or altering a computer system or a data carrier.

(2) The attempt shall be punishable.

The modifications of the German criminal code are reflected in the following: firstly, modification about article 202a, adding 202b and 202c as the following items of 202a, and the ligation provision related to the article 202, the article 205, was further modified in response to article 202. 202a regulates illegal activities of Data Espionage, 202b stipulates the crime of intercepting data, and 202c refers to the illegal activities of preparation for snooping or intercepting computer data. Secondly, this amendment modified the article 303a, 303b and the ligation item 303c that is related to 303a and 303b.[178] The content of 303a concerns the crime of Alteration of Data, 303b stipulates the crime of Computer Sabotage, which includes physically destroying a computer and by means of indirectly affecting a computer to make it inoperable; and 303c stipulates the crime under 202b would be punished with the condition that offenders have been sued in court. At present, the accusations about cyber crime in German legislation include prying into data, intercepting data, preparing to spy and intercept data,

[178]Pi Yong, The German Cyber Crime Legislation against the Background of Integration of European Criminal Law. Peking University Law Journal, Vol.23，No.5 (2011), p. 1038-1060.

modifying data, destroying a computer and cyber crime by means of a computer and the internet.

2.3 Legislation of Austria

As a central European country, Austrian organized crime has a close relationship with its neighbors' OCGs, such as Italy and some eastern countries. The legislation of Austria against OC and cyber crimes will be introduced as follows.

2.3.1 Legislation of Austria against Organized Crime

Austrian law against OC can be found in the Security Police Act and Criminal Code. In the third part, art. 16 sec. subpar 2 of the Security Police Act the term "general danger" is described:[179]

1. In the event of a dangerous attack (sec. 2 and 3) or
2. As soon as three or more persons get together with the intention of repeatedly committing criminal acts punishable by the court (gang or organized crime).

Except for the Security Police Act, from the perspective of this dissertation,[180] the article 278 (criminal association), 278a (criminal organization), 278b (terrorist association) and 279 (armed association) of the Criminal Code of Austria are the basic provisions against organized crime. As a matter of fact, the evolution of legislation

[179] Maximilian Edelbacher, Organized Crime in Austria-Vienna: The Gateway to The East, In *Organized Crime: A World Perspective*, Third International Police Executive Symposium, Kanagawa University, Yokohama, Japan Nov 28-Dec 1, 1996, The Society of Law, University of Kanagawa, Vol.31, No. 3, 1997, p.329.

[180] This dissertation takes a broad definition concerning organized crime, it covers whatever the criminal association or organization by which the criminals are connected together, who can commit all types of crimes with any aims.

against organized crime experienced the following processes[181]: criminal organization under §278a was established by the amendment of the criminal code in 1993. After that, §278a obtained its present basic form by amendment of the criminal code in 1996, it came into force on 1.3.1997. In 2002 the definition of criminal organization was established by amendment of the criminal code 2002.

2.3.2 Legislation of Austria against Cyber Crime

Legislation of Austria against cyber crime can be found in its Specific Provisions of the Criminal Code. (1) In chapter 5, invasion of privacy and particular professional confidence, the article 118a stipulates the crime of illegally attacking a computer system, and the article 119 regulates invasion of telecommunication secrets and intercepting abusive data.[182] (2) Under chapter 6, illegal activities of invading another person's property rights, the article 126a, 126b and 126c concerns cybercrime. The article 126a regulates the crime of damaging data, the article 126b stipulates the crime of disturbing the functions of a computer system, and article 126c is the crime of abusing computer programs or passwords. The article 148a under the chapter concerns the crime of abusing and processing fraudulent data.[183] (3) In chapter 10, illegal activities concerning sex, the article 207a stipulates the crime of displaying child pornography. Even though this article does not mention that this crime can be committed by means of a computer, a reasonable extensive interpretation of the wording of this item, can be applied to this type of crime via the internet.[184] (4) Under chapter 12, illegal activities of forging documents and evidence, the article 225a is a stipulation about the crime of

[181] Susanne Reinde-Krauskopf and Farsam Salimi, Retrieved on 01.August.08 from http: //www.parlament.gv.at/PAKT/VHG/XXIV/III/III OO348/fname 263545.pdf.
[182] See The Criminal Code of Austria.
[183] Ibid.
[184] Ibid.

forging data.[185] (5) The article 51 of the Data protection Act also protects personal data, it states[186]:

> Whoever intends to gain a pecuniary advantage or to inflict damage to personal data, which is
>
> either exclusively entrusted to him by virtue of his professional employment;
>
> or becomes accessible
>
> or which he has procured illegally, or even used, or makes it available to another;
>
> even though this data is of legitimate interest and confidential to the victim,
>
> then, if the act is not punishable under any other provision of stringent punishment, the court should punish the act with imprisonment of up to one year.
>
> The offender shall be prosecuted only with the authorization of the victims.

2.4 Legislation of France

As a member of the European Union, France also has legislations against organized crimes and cyber crimes, but it does not have particular legislations against cyber transnational organized crimes. In the following text legislations concerning these two types of crimes will be introduced respectively.

2.4.1 Legislation of France against Organized Crime

[185] Ibid.
[186] On-line resources, retrieved on 10.Aug.2014 from http://www.ris.bka.gv.at/Ergebnis.wxe?Suchworte=datenschutzgesetz+51&Abfrage=Gesamtabfrage&x=10&y=7.

Under the Criminal Code of France, the article of 405-1 stipulates the crime of participating in evildoers' association.[187] It states: whoever intentionally carries out one or several felonies, or one or several misdemeanors, should be sentenced to ten years' imprisonment, and any cliques or tacit agreements arising therefrom constitute the crime of participating in an evildoers' association.[188]

In respect of money laundering, there are a great number of laws and acts against this crime. The article 335-5 of the Criminal Code of France criminalizes the conduct of laundering dirty money from prostitution. An ordinance in 1987 was adopted to implement the article L.627 of the Public Health Law, which regulates laundering illegal income from illegal drug activities. The Customs Law of 1988 defines the illegal conduct of international money laundering. The 90-614 Act of 1990 (also named Anti-money Laundering Act) sets the role and duty of financial institutions during the process of laundering money from illegal drug business. In 1993 the 93-122 Act expands the duty of financial institutions in anti-money laundering from the scope of drug businesses to OCGs.[189] In 1994, four acts were further adopted by the French Parliament, which comprehensively revised the Criminal Code, absorbed article L.127 (concerning laundering dirty money from drug businesses) as the article 222-38 of Criminal Code, and adjusted the article 335-5 of old Criminal Code as the article 225-6 of new Criminal Code. In 1996, the 96-392 Act[190] further added two accusations, respectively, general money laundering and aggravated money laundering.[191]

2.4.2 Legislation of France against Cyber Crime

[187] Cited in Lu Jianping eds. *Comparative Study of Organized Crime,* Law Press • China, 200, P.53.
[188] Lu Jianping eds. *Comparative Study of Organized Crime,* Law Press • China, 2004, P.53-54.
[189] Ordinace of 1987, the Customs Law of 1988, the 90-614 Act of 1990 and the 93-122 Acts are still effective in France.
[190] 96-392 Act still have binding force at present.
[191] Ibid.

France's Ratification of the Council of Europe Convention on Cybercrime was made on 10.January.2006, amended as Law no.2004-575 of June 21. 2004, and entered into force on June 23. 2004. In France cyber crimes are mainly categorized into the following types[192]: (1) the article 323-1 regulates: Fraudulent accessing or remaining within all or part of an automated data processing system is punished by a sentence not exceeding two years' imprisonment and a fine of 30.000 euro; Where this behavior causes the suppression or modification of data contained in that system, or any alteration of the functioning of that system, the sentence is not exceeding three years' imprisonment and a fine of 45.000 euro. (2) The article 323-2: Obstruction or interference with functioning of an automated data processing system is punished by a sentence not exceeding five years' imprisonment and a fine of 75.000 euro. (3) The article 323-3 states: Fraudulent introduction of data into an automated data processing system or fraudulent suppression or modification of the data that it contains is punished by a sentence not exceeding five years imprisonment and a fine of 75.000 euro. (4) Article 323-3-1: Fraudulently, and without legitimate motive, importing, holding, offering, selling or making available any equipment, tool, computer program or any data designed or particularly adapted to commit one or more offences provided for by articles 323-1 to 323-3, is punishable by the sentences prescribed for offences in preparation or the one that carries the heaviest penalty (5) Article 323-4: Participation in a group or conspiracy established with a view to preparation of one or more offences set out under articles 323-1 to 323-3, and demonstrated by one or more material actions, is punished by the penalties prescribed for offences in preparation or one that carries the heaviest penalty.

2.5 Legislation of the United Kingdom

[192] On-line resources, retrieved on 10.Aug.2014 from http://www.cybercrimelaw.net/France.html.

Even though the United Kingdom is a country with tradition of common law, it also has written law against OC and cyber crimes. These legislations are rapidly developing during the recent 10 years, and they will be briefly introduced in the following section.

2.5.1 Legislation of the United Kingdom against Organized Crime

Before the 21st century, no definition of OCGs existed in the criminal law of Britain. In judicial practice, law enforcement usually treated this type of crime as conspiracy under the Criminal Code of Britain of 1977. Along with the situation of OC becoming much more serious, which directly lead to a great boom in legislation combating OC in the 21st century, this can be reflected in three legislative documents, including Proceeds of Crime Act of 2002, A Defeat Strategy of Organized Crime in the 21st Century and the Serious Organized Crime and Police Act of 2005.[193] These legislative documents stipulate many new accusations about OC, and meanwhile confer a much broader power of enforcing the laws on law enforcement agencies.

2.5.2 Legislation of the United Kingdom against Cyber Crime

The legislation of Britain against cyber crime can be defined as having five aspects.[194] Firstly, the Data Protection Act of 1984.[195] It generalizes the contents of data protection, such as the data protection of individuals, enhancement of standardizing data-processing and prevention of abusing a computer and its resources; Secondly, the Police and

[193] Zhao Chi. The Investigation of British Legislation against Organized Crime, *International Research*, Issue 403 (2013).
[194] These five aspects'of legislation are still effective now.
[195] Yang Jianzheng, the Legislation of Computer Law within Worldwide, Journal of Zhengzhou University, Issue 5 (1999).

Criminal Evidence Ordinance of 1984.[196] It makes explicit stipulations about whether computer documents can be considered as criminal evidence of crimes and revealing criminal facts during the criminal procedure; Thirdly, the Computer Misuse Act of 1990.[197] It stipulates four types of crimes, respectively, unauthorized access to computer material, unauthorized access with intent to commit or facilitate commission for further offences, unauthorized acts with intent to impair, or with recklessness as to impair the, operation of a computer, etc. And making, supplying or obtaining articles for use in offences under section 1 or 3. The part 5 sections 35-38 of The Police and Justice Act 2006 Chapter 48 amends the Computer Misuse Act, which came into force in 2008. As follows[198]:

35 Unauthorized access to computer material: (1) In the Computer Misuse Act 1990 (c. 18) ("the 1990 Act"), section 1 (offence of unauthorized access to computer material) is amended as follows. (2) In subsection (1)- (a) in paragraph (a), after "any computer" there is inserted ", or to enable any such access to be secured"; (b) in paragraph (b), after "secure" there is inserted ", or to enable to be secured,". (3) For subsection (3) there is substituted- "(3) A person guilty of an offence under this section shall be liable- (a) on summary conviction in England and Wales, to imprisonment for a term not exceeding 12 months or to a fine not exceeding the statutory maximum or to both; (b) on summary conviction in Scotland, to imprisonment for a term not exceeding six months or to a fine not exceeding the statutory maximum or to both; (c) on conviction or indictment, to imprisonment for a term not exceeding two years or to a fine or to both."

36 Unauthorized acts with intent to impair the operation of a computer, etc: For section 3 of the 1990 Act (unauthorized modification of computer material) there is substituted-"3 Unauthorized acts with intent to impair, or with recklessness as to impairing, operation of computer, etc. (1) A person is guilty of an offence if- (a) he does any unauthorized act in relation to a computer; (b) at the time when he does the act he knows that it is unauthorized; and (c) either subsection (2) or

[196] Liu Shoufen and Fang Shuxin. Analyzing Eight Countries' Legislation Against Cyber Crime and their Enlightenment to the Legislation of China, Law Science Magazine, Volume 25, (15.09.2004).
[197] Ibid.
[198] On-line resources, retrieved on 22.Aug.2014 from http://www.cybercrimelaw.net/UK.html.

subsection (3) below applies. (2) This subsection applies if the person intends by doing the act- (a) to impair the operation of any computer; (b) to prevent or hinder access to any program or data held in any computer; (c) to impair the operation of any such program or the reliability of any such data; or (d) to enable any of the things mentioned in paragraphs (a) to (c) above to be done. (3) This subsection applies if the person is reckless as to whether the act will do any of the things mentioned in paragraphs (a) to (d) of subsection (2) above. (4) The intention referred to in subsection (2) above, or the recklessness referred to in subsection (3) above, need not relate to- (a) any particular computer; (b) any particular program or data; or (c) a program or data of any particular kind. (5) In this section- (a) a reference to doing an act includes a reference to causing an act to be done; (b) "act" includes a series of acts; (c) a reference to impairing, preventing or hindering something includes a reference to doing so temporarily. (6) A person guilty of an offence under this section shall be liable- (a) on summary conviction in England and Wales, to imprisonment for a term not exceeding 12 months or to a fine not exceeding the statutory maximum or to both; (b) on summary conviction in Scotland, to imprisonment for a term not exceeding six months or to a fine not exceeding the statutory maximum or to both; (c) on conviction on indictment, to imprisonment for a term not exceeding ten years or to a fine or to both."

37 Making, supplying or obtaining articles for use in computer misuse offences: After section 3 of the 1990 Act there is inserted- "3A Making, supplying or obtaining articles for use in offence under section 1 or 3 (1) A person is guilty of an offence if he makes, adapts, supplies or offers to supply any article intending it to be used to commit, or to assist in the commission of, an offence under section 1 or 3. (2) A person is guilty of an offence if he supplies or offers to supply any article believing that it is likely to be used to commit, or to assist in the commission of, an offence under section 1 or 3. (3) A person is guilty of an offence if he obtains any article with a view to its being supplied for use to commit, or to assist in the commission of, an offence under section 1 or 3. (4) In this section "article" includes any program or data held in electronic form. (5) A person guilty of an offence under this section shall be liable- (a) on summary conviction in England and Wales, to imprisonment for a term not exceeding 12 months or to a fine not exceeding the statutory maximum or to both; (b) on summary conviction in Scotland, to imprisonment for a term

not exceeding six months or to a fine not exceeding the statutory maximum or to both; (c) on conviction on indictment, to imprisonment for a term not exceeding two years or to a fine or to both."

38 Transitional and saving provision (1) The amendments made by- (a) subsection (2) of section 35, and (b) paragraphs 19(2), 25(2) and 29(2) of Schedule 14, apply only where every act or other event proof of which is required for conviction of an offence under section 1 of the 1990 Act takes place after that subsection comes into force.(2) The amendments made by- (a) subsection (3) of section 35, and(b) paragraphs 23, 24, 25(4) and (5), 26, 27(2) and (7) and 28 of Schedule 14, do not apply in relation to an offence committed before that subsection comes into force. (3) An offence is not committed under the new section 3 unless every act or other event proof of which is required for conviction of the offence takes place after section 36 above comes into force. (4) In relation to a case where, by reason of subsection (3), an offence is not committed under the new section 3- (a) section 3 of the 1990 Act has effect in the form in which it was enacted; (b) paragraphs 19(3), 25(3) to (5), 27(4) and (5) and 29(3) and (4) of Schedule 14 do not apply. (5) An offence is not committed under the new section 3A unless every act or other event proof of which is required for conviction of the offence takes place after section 37 above comes into force. (6) In the case of an offence committed before section 154(1) of the Criminal Justice Act 2003 (c. 44) comes into force, the following provisions have effect as if for "12 months" there were substituted "six months"- (a) paragraph (a) of the new section 1(3);(b) paragraph (a) of the new section 2(5); (c) subsection (6)(a) of the new section 3; (d) subsection (5)(a) of the new section 3A. (7) In this section- (a) "the new section 1(3)" means the subsection (3) substituted in section 1 of the 1990 Act by section 35 above; (b) "the new section 2(5)" means the subsection (5) substituted in section 2 of the 1990 Act by paragraph 17 of Schedule 14 to this Act; (c) "the new section 3" means the section 3 substituted in the 1990 Act by section 36 above; (d) "the new section 3A" means the section 3A inserted in the 1990 Act by section 37 above.

Fourthly, the Regularity, Report and Responsibility of Internet Security Rules,[199] This rule aims to eliminate child pornography and other harmful information on the internet. Finally, in order to punish other crimes related to a computer or the internet, Juvenile

[199] Ibid.

Law, Video Product Act, Prohibiting Universal Use Computer Act and the Criminal Justice and Public Order Amendment are also usually used to deal with these crimes.[200]

3. Legislation of China

At present, almost all the official documents do not recognize that there are mafia-types of criminal groups existing in China, but the existence of so-called underground organizations or criminal gangs is universally accepted by judicial practices. However, a great number of scholars in the circle of criminal law hold the opinions that mafia-type of OCGs is developing in mainland of China.[201] In the following legislations of China against OC and cyber crimes will be briefly introduced.

3.1 Legislation of China against Organized Crimes

The legislations of Hong Kong, Macau and Taiwan are different from that of mainland China, so in this part, the legislations of the mainland and the legislations of the other three regions will be respectively introduced.

3.1.1 Legislation of Mainland

[200] Liu Wei, Introduction of Foreign Prevention and Control System of Cyber Crime, *Netinfo Security*, Issue 6 (2005).
[201] Chen Xingliang, Organized Crime or Criminal Organizations-Rationalistic Thinking of the Criminal Organizations with the Underground Gang Characteristics, issued in the Compilation of Annual Theses of China Law Science Association of Criminal Law in 2002, p.1008-1013.

Under the Criminal Code of China of 1997, the article 294 provides the crime with characteristics of underground gang, which includes three types of accusations, respectively, the crime of organizing, leading or participating in criminal organizations with the characteristics of an underground gang, the crime of entering into Chinese territory to develop the membership of organized criminal groups, and the crime of harboring, or conniving in criminal organizations with characteristics of underground gang.[202] After 1997, in 2000 and 2002 some judicial interpretations were adopted to aid the application of article 294 in judicial practice. Article 120 stipulates two kinds of crimes concerning terrorism, namely, the crime of organizing, leading or participating in terrorist groups and the crime of supporting terrorist activities.[203]

In respect of legislation against money laundering, firstly, the article 191 of the Criminal Code of 1997 provides for money laundering, but its predicated offences only include drug crime, the crime of criminal organization with characteristics of an underground gang and contraband crime. In 2001, the third Amendment of the Criminal Code of China revised article 191. On the basis of the original three predicated offences, the other four types of predicated offences were added to formulate the new article 191. And these four predicated offences include the crime of bribery and corruption, the crime of terrorist activities, the crime of destroying the order of financial management, and the crime of financial fraud. So the new article 191 includes 7 types of predicated offences about money laundering.[204] Secondly, in 2003 some rules were adopted to assist anti-money laundering, including Anti-money Laundering Provisions of Financial Institutions, Measures for the Management of Reporting Large Amounts and Suspicious Payment Transactions with RMB and Measures for the Management of Reporting Large Amounts and Suspicious Foreign Exchange Transactions of Financial Institutions.

[202] See Criminal Code of China.
[203] Ibid.
[204] Ibid.

3.1.2 Legislation of Hong Kong

OC in Hong Kong are often related to Hong Kong Triads. The chapter 151 of the Societies Ordinance, which lists all crimes concerning OCGs, such as the crime of imitating a member of Triad, the crime of sponsoring or assisting Triad (the item 1 of article 20), the crime of claiming to be a member of Triad and the crime of possessing, keeping and controlling the articles of Triad (the item 2 of article 20), the crime of managing illegal societies (the article 19), the crime of permitting illegal societies gathering at dwelling places (the article 21), and the crime of impelling others to finance illegal societies (the article 23).[205] Besides the Societies Ordinance, in 1994, the governor of Hong Kong enacted the Organized and Serious Crimes Ordinance with the purpose of "creating new powers of investigation into organized crimes and certain other offences and into the proceeds of the crimes of certain offenders, providing for the confiscation of the proceeds of crime; making provision in respect of the sentencing of certain offenders; creating an offence of assisting a person to retain the proceeds of crime; and for ancillary and connected matters".[206] Legislation of anti-money laundering is stipulated under the Organized and Serious Crimes Ordinance and Drug Trafficking Ordinance.

3.1.3 Legislation of Macau

[205] Lu Jianping eds. *Comparative Study of Organized Crime*, Law Press • China, 2004, P.46-47.
[206] He Bingsong, Organized Crime and Its Containment in China, In *Organized Crime: A World Perspective*, Third International Police Executive Symposium, Kanagawa University, Yokohama, Japan Nov 28-Dec 1, 1996, The Society of Law, University of Kanagawa, Vol.31, No. 3, 1997, p.80.

In 1978, Macau enacted (1/78/M Act), a particular criminal law against OC, which focuses on combating and punishing underground criminal organizations in Macau. Its Clause 2 defines the conception of underground societies. In 1997, the 6/97/M Act was enacted, which is also named the Organized Crime Law. It stipulates 10 types of crimes, i.e., the crime of underground society (article 2), extortion under the name of protecting (article 3), the crime of claiming to be an underground society (article 4), the crime of improperly detaining certification of others (article 6), international trafficking in persons (article 7), the crime of manipulating prostitution (article 8), the crime of harassing others in a public place (article 9), the crime of shifting, transferring or covering up illegal property or goods (article 10), illegal gambling in combined groups (article 11), and the crime of violating judicial secrecy (article 13).[207] In 1998, the 24/98/M Act was enacted to supplement the article 10 of Organized Crime Law to counter money laundering.[208]

3.1.4 Legislation of Taiwan

There is no particular stipulation concerning underground organizations and OC in the Criminal Law of Taiwan. However, in judicial practice, article 154 of the Criminal Law of Taiwan is used to deal with OC. It is aimed at the crime of forming a criminal society. Except article 154 of Criminal Law, the Inspecting and Eliminating Gangsters Ordinance of 196 and Organized Crime Prevention Act of 1996 were also enacted to counter organized crime.[209]

[207] On-line article (2013), The General Situation of Legislation of Macau against Organized Crime. Retrieved on 10.Sept. 2013 from http://www.chinalawedu.com/new/201211/wangying20121116203042450462 64.shtml.
[208] 1/78/M Act, 6/97/M Act and 24/98/M Act are still effective now.
[209] Xu Jieqing (2006). *A Study of Organized Crime in Taiwan District and the Countermeasures*. Chinese Procuratorial Press, p.259-263.

3.2 Legislation of Mainland against Cyber Crime

Under the Criminal Code of China of 1997, three articles are related to cybercrime, respectively, article 285, 286 and 287. Five types of crimes and a special rule are stipulated under these articles. Firstly, under article 285 there are four crimes, the crime of unlawfully trespassing in the computer system, the crime of illegally obtaining the data ofa computer information system, the crime of illegally controlling a computer information system, and the crime of providing programs or instruments to trespass or unlawfully control a computer information system. Secondly, the article 286 stipulates the crime of destroying a computer information system. Thirdly, the article 287 is a special rule of cyber crime, which states that carrying out financial fraud, theft, embezzlement, embezzlement of public funds, stealing state secrets and other crimes by means of a computer or the internet, the offender should be convicted and punished in accordance with the relevant provisions of this Code.[210]

4. Legislation of Russia

Under Russian legislations, there is still no particular law against cyber transnational organized crime. In the following section the legislation of Russia against OC and cyber crimes will be introduced.

4.1 Legislation of Russia against Organized Crime

[210] See The Criminal Code of China.

Legislation of Russia against OC can be introduced from three aspects. Firstly, the Criminal Code of Russia,[211] under criminal code, article 35 defines criminal organized gangs and OCGs, article 210 stipulates the crime of establishing, leading or participating in OCGs, and there are more than 70 articles regarding crimes committed by OCGs which are used to be the enhancing liability element of crime constitution, such as item 7 of paragraph 2 of article 105.[212] Secondly, a particular law to counter organized crime, the Anti-organized Crime Law, was not enacted in the end. However, it defined many concepts related to organized crime, and provided a lot of useful measures against organized crime. Thirdly, among the other laws, except for the criminal code, there are 5 other laws countering organized crime, including the Anti-money Laundering Act, the Witness Protection Act, the Anti-terrorism Act, the Tracking down and Arresting Activities Act and the Anti-corruption Act.[213]

4.2 Legislation of Russia against Cyber Crime

Under The Criminal Code of Russia, there are 3 articles stipulating cyber crimes. These three articles are crimes of targeting a computer, namely, the crime of accessing, altering or blocking the information of a computer system without authority (article 272), the crime concerning malicious programs (article 273) and the crime of targeting the internet or maliciously utilizing a computer internet. Of course, there are other articles existing in the Criminal Code of Russia to counter computer or cyber crime, but they do not directly target the technologies that are used to commit crimes; in other

[211] Lu Jianping eds. *Comparative Study of Organized Crime*, Law Press • China, 2004,P.56.

[212] Cui Man, Research on the Organized Crime in Russia, On-line dissertation. Retrieved on 15.Sept. 2013 from http://epub.cnki.net/kns/detail/detail.aspx?QueryID=3&CurRec=1&recid=&FileName=2009087424.nh&DbName=CDFD0911&DbCode=CDFD&pr=.

[213] Ibid.

words, for these crimes, a computer and the internet are just used as instruments for committing the corresponding crimes.[214]

5. Legislation of Japan

As compared to neighboring China, the level of Japanese OC is more advanced than in China. In order to analyze the situation of Japanese present legislation countering organized crime in the context of the internet, the legislation of Japan against OC and cyber crimes will be briefly introduced in the following section.

5.1 Legislation of Japan against Organized Crime

There are three laws[215] being used to combat OC in Japan, respectively, the Yakuza Countermeasure Act of 1991, the Disruptive Activities Prevention Act of 1952 and the Organized Crime Countermeasure Act.[216] The contents of the Yakuza Countermeasure Act include the establishment of a Public Security Committee, designation of Yakuza, effectiveness of the designation, cutting off the social demand and human resources of certain Yakuza, etcetera. The Disruptive Activities Prevention Act mainly targets the regulation of terrorism activities, like arson attacks and murder. The Organized Crime Countermeasure Act concerns stipulations of aggravation of penalty of organized crime, money laundering and some measures to detect organized crime, etc.[217]

---

[214] Feng Chaohui and Huang Qingsheng, Comparison of Anti-cyber Crime Law between Different Countries, Network Security Technology and Application,(02.2006).

[215] These three laws, i,e., the Yakuza Countermeasure Act of 1991, the Disruptive Activities Prevention Act of 1952 and the Organized Crime Countermeasure Act, are still effective at present.

[216] Xu Jieqing, (2006), *a Study of Organized Crime in Taiwan District and the Countermeasures*, Chinese Procuratorial Press, p.68-70.

[217] Ibid.

5.2 Legislation of Japan against Cyber Crime

Legislation of Japan against cyber crime includes Unauthorized Computer Access Law and Penal Code. The former came into effect on February 3, 2000, and the main content includes[218]: (1) Article 3, Prohibition of acts of unauthorized computer access:- no person shall conduct an act of unauthorized computer access. The act of unauthorized computer access means an act that falls under one of the following items: (a) An act of making available a specific use which is restricted by an access control function by taking control of a specific computer having that access control function through inputting into that specific computer, via a telecommunication line, another person's identification code for that access control function (to exclude such acts conducted by the access administrator who has added the access control function concerned, or conducted with the approval of the access administrator concerned or of the authorized user for that identification code); (b) An act of making available a restricted specific use by taking control of a specific computer having that access control function through inputting into it, via a telecommunication line, any information (excluding an identification code) or command that can evade the restrictions placed by that access control function on that specific use (to exclude such acts conducted by the access administrator who has added the access control function concerned, or conducted with the approval of the access administrator concerned; the same shall apply in the following item); (c) An act of making available a restricted specific use by taking control of a specific computer, whose specific use is restricted by an access control function installed into another specific computer which is connected, via a telecommunication line, to that specific computer, through inputting into it, via a telecommunication, any information or command that can evade the restriction

[218] On-line resources, retrieved on 22.Aug.2014 from http://www.cybercrimelaw.net/Japan.html.

concerned. (2) Article 4, Prohibition of acts of facilitating unauthorized computer access, No person shall provide another person's identification code relating to an access control function to a person other than the access administrator for that access control function or the authorized user for that identification code, in indicating that it is the identification code for that computer's specific use, or at the request of a person who has such knowledge, excepting the case where such acts are conducted by that access administrator, or with the approval of that access administrator or of that authorized user. (3) Penal provisions: (a) Article 8, A person who falls under one of the following items shall be punished with penal servitude for not more than one year or a fine of not more than 500,000 yen: (1) A person who has infringed the provision of Article 3, paragraph 1; (b) Article 9. A person who has infringed the provision of Article 4 shall be punished with a fine of not more than 300,000 yen.

Under Penal Code: (1) Article 258, Damage to Documents in Public Use, a person who damages documents or electronic-magnetic records in public official use shall be punished with imprisonment for not less than three months or more than seven years; (2) Article 259, Damage to Documents in Private Use, a person who damages documents or electro-magnetic record in private use and owned by another person who proves a right or duty shall be punished with imprisonment for not more than five years.[219] However, by means of amending the Penal Code, Japan improved the legislation against cyber crime. Five aspects are included in this amendment: (1) Adding the definition of electromagnetic recording as the supplement of the item 2 of article 7.[220] (2) Revising the corresponding chapter of criminal code concerning false documents, supplementing stipulation concerning the protection of electromagnetic recording to prevent data that would be illegally operated.[221] (3) supplementing the crime of obstructing computer

[219] On-line resources, retrieved on 22.Aug.2014 from http://www.cybercrimelaw.net/Japan.html.
[220] Liu Shoufen and Fang Shuxin. Analyzing Eight Countries' Legislation Against Cyber Crime and their Enlightenment to the Legislation of China, Law Science Magazine, Volume 25, (15.09.2004).
[221] Ibid.

operation (the item 2 of article 234), which includes the following crimes: damaging a computer or records stored in the computer, inputting fake data or false order into another's computer, or using the other means to prevent the computer from being used for its original purposes.[222] (4) Supplementing the crime of internet fraud with computer (the item 2 of article 246).[223] (5) Supplementing the crime of ruining electromagnetic recording.[224]

6. Regional and international Conventions against Cyber Transnational Organized Crime

Apart from the legislations of different countries against OC and cyber crime, at the level of regional and international, there are certain conventions against these crimes.

At the regional level, on the one hand, the Council of Europe adopted certain treaties to investigate OC, such as the European Convention on Mutual Assistance in Criminal Matters and its Additional Protocols (1959) and the European Convention on Laundering, Search, Seizure and Confiscation of the Proceeds of Crime (1990).[225] On the other hand, in order to combat cyber crime, the Council of Europe adopted the Convention on Cybercrime of Europe of 23.11.2001, and the European Commission proposed Directive 2013/40/EU of the European Parliament and of the Council of 12

[222] Ibid.
[223] Ibid.
[224] Ibid.
[225] Cyrille Fijnaut and Letizia Paoli, The Initiatives of the European Union and the Council of Europe, In Cyrille Fijnaut and Letizia Paoli (ed.) (2004), *Organized Crime in Europe: Concepts Patterns and Control Policies in the European Union and Beyond*, Springer, p.48.

August 2013 on attacks against information systems and replaced Council Framework Decision 2005/222/JHA.[226]

At the international level, there are the United Nations Convention against Transnational Organized Crime and some protocols against specific TOC. The latter include Protocol against the Smuggling of Migrants by Land, Sea and Air, supplementing the UN Convention against Transnational Organized Crime, the Protocol to Prevent, Suppress and Punish Trafficking in Persons, Especially Women and Children, supplementing the United Nations Convention against Transnational Organized Crime, the Optional Protocol to the Convention on the Rights of the Child on the sale of children, child prostitution and child pornography, the United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances of 1988 and the United Nations Convention against Corruption, etc.

7. Legislative Absences and Judiciary Obstacles when Fighting against Cyber Transnational Organized Crime

On the basis of the examination of certain countries' legislations, regional and international conventions prevent the trend of interaction and integration of transnational organized crime and cybercrime; in other words, cyber transnational organized crimes. Obviously, the traditional criminal theories about transnational organized crime have been overtaken by this trend. So in the following section legislative absence and judiciary obstacles will be analyzed.

[226] Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA, Official Journal of the European Union, 14.Augest.2013.

7.1 Legislative Absences and Loopholes

The nature of hysteresis quality always accompanies every law since at the moment when they are enacted, the legislations against TOC and cyber crimes are also no exception. When the internet affected the laws against TOC and cyber crime, there would be legislative absence and loopholes within those existing laws.

7.1.1 Absences of Regional and International Convention against Cyber Transnational Organized Crime

At the international level, the UNTOC and some protocols target particular TOC, but there has been no convention specifically against CTOC. At the regional level, taking Europe as an example, there is no convention particularly combating organized crime, but the existing European Convention on Mutual Assistance in Criminal Matters and its Additional Protocols (1959) and the European Convention on Laundering, Search, Seizure and Confiscation of the Proceeds of Crime (1990). And in order to combat cyber crime, the Council of the European Union adopted the Convention on Cybercrime of Europe of 23.11.2001, and the European Commission proposed Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on Attacks against Information Systems.[227] Except these regional and international documents, there are no particular regional and international legal documents to combat cyber transnational organized crime. Furthermore, these existing conventions and protocols are insufficient to cope with the transnational organized crime in the internet age. In this part only the absences and loopholes of the United Nations Convention against Transnational Organized Crime and the Council of Europe Convention on

[227] It replaced the EU Council Framework Decision 2005/222/JHA on Attacks against Information System of 24.2.2005.

Cybercrime will be analyzed, and only the provisions of these two documents related to the main theme of this dissertation are analyzed, namely, the provisions of criminal jurisdiction and the scope of TOC and cyber crime under these two documents.

Firstly, in the aspect of criminal jurisdiction, article 15 of the United Nations Convention against Transnational Organized Crime stipulates jurisdiction.[228] It stipulates territorial criminal jurisdiction, personal criminal jurisdiction and protective criminal jurisdiction. And article 22 of the Council of Europe Convention on Cybercrime is concerning jurisdiction, but it only stipulates territorial criminal jurisdiction and personal criminal jurisdiction.[229] These are just recapitulative stipulations about the jurisdiction of transnational organized crime and cyber crime, and they do not clearly define the principle of determining the scope of locations of criminal acts, criminal consequences and criminal purposes. In other words, there is no specific stipulation which can be used to solve the positive conflicts and the negative conflicts of the jurisdiction of CTOC and cyber crime. In chapter 5 of this dissertation, how to solve these problems and what kind of rule can be used will be discussed in detail.

Secondly, there is the scope of transnational organized crime and cyber crime. According to the UNTOC, the article 3 of this convention regulates the scope of TOC. In line with it, the type of TOC includes the crimes which are stipulated by article 5, article 6, article 8 and article 23, the definition of serious crime is stipulated in article 2 of this convention.[230] Even though article 2 can be considered as a miscellaneous provision about TOC, it means as long as transnational crimes were committed by OCGs, whatever the type of these crimes, they should be criminalized as TOC. Of course, there would be a way, by means of reasonably extensive interpretation, for those

[228] See The United Nations Convention against Transnational Organized Crime.
[229] See The Council of Europe Convention on Cybercrime.
[230] See The United Nations Convention against Transnational Organized Crime.

cyber crimes or traditional crimes, related to ICTs and committed by transnational organized criminal groups, to be included in the scope of transnational organized crime. However, on the one hand, the effect of combating cyber transnational organized crime would be much better if there were specific articles or provisions defining and dealing with CTOC in this convention. On the other hand, it is also a problem whether it is reasonable or not that this convention can be applied to cyber transnational organized crime. Probably, the answer is not, since the CTOC has certain characteristics different from TOC. Even though extensive interpretation can be used to expand the application scope of the UNTOC, these problems cannot be solved completely. At least in the internet age the provisions about the scope, and jurisdiction of TOC should be revised under the UNTOC. In accordance with the Council of Europe Convention on Cybercrime, the scope of cyber crime is much narrower, and four categories of cyber crime are stipulated in this convention, respectively, offences against confidentiality, integrity and availability of computer data and systems, computer-related offences, content-related offences and offences related to infringements of copyright and related rights.[231] From article 2 to article 10, 9 types of criminal act are regulated in section 1 of chapter 2 of this convention, including illegal access, illegal interception, data interference, system interference, misuse of devices, computer-related forgery, computer-related fraud, offences related to child pornography and offences related to infringements of copyright and related rights. The loopholes of these articles include two points: a. the scope of cyber crime is too narrow, as manifested in the aspect of the other traditional crimes which happened in cyberspace but are not included; b. the absences of provisions concerning joint offenders of these cybercrimes, For example, transnational organized criminal groups (TOCGs) are also likely to commit cybercrimes. So once cybercrimes are committed by such TOCGs, there would be no available provisions to be used to punish them according to joint criminal theory. Because this convention does not touch on OCGs and TOCGs which are involved in these types of cybercrimes, the only available provisions which can be used to punish OCGs are those

[231] See The Council of Europe Convention on Cybercrime.

clauses providing criminal theory, which deal with single offenders under this convention. Accordingly, as a matter of fact, this means that the criminal responsibilities of the organized criminal groups they have taken, were not compatible with the ones they should take.

7.1.2 Loopholes and Weaknesses of Domestic Law

The above parts of this section examined legislations against organized crime and cyber crime of some European, Asian and North American countries. The loopholes can be found through comparing the legislative forms of these countries, and based on an analysis of these legislative forms, three types can be concluded:

- The form of special legislation. This means that the law-making organ of a certain country enacted special laws to combat OC. This category includes the legislation of the USA, the UK, Hong Kong, Macau and Taiwan. On the one hand, even though the form of special legislation against OC is more systematic and detailed, they are still unable to combat CTOC. For example, if the OCGs utilize the internet or other ICTs to commit TOC, namely CTOC, and since the internet has changed the nature of this type of crime, these legislations are unable to deal with joint crime and criminal jurisdiction under CTOC. On the other hand, legislations of these countries against cyber crime do not provide relative provisions directed against OCGs committing cyber crimes.

- The form of criminal code. It means that there are articles directed against OC under specific provisions of the criminal code. The mainland of China, Austrian and Russian legislations against organized crime fall into this category. The criminal code targets regulate all sorts of crime as a whole, so it is difficult to adopt special procedural provisions concerning organized crime. This legislative form is also

insufficient to deal with joint crime and criminal jurisdiction under cyber transnational organized crime.

- The combined form. It means that not only does the criminal code have articles against organized crime, but also criminal procedure law and the other specific criminal laws set provisions to combat organized crime. The legislations of Italy, Germany and Japan belong to this category. Even though this form of legislation against organized crime is the most detailed among these three categories, both legislations against organized crime, and cyber crime, do not pay enough attention to the trend of interaction and integration of OC and cyber crime; in other words, they are short of relative articles and provisions to deal with joint crime and criminal jurisdiction under cyber transnational organized crime.

Generally speaking, on the one hand, even though the authorities of a majority of countries have recognized the seriousness of CTOC, until now there has been no country which has adopted a specific criminal law against cyber organized crime or cyber transnational organized crime. Of course, under the present circumstances, probably it is enough that most countries can deal with this type of crime by means of their criminal codes and corresponding law against cybercrime. However, in the future, if CTOC become much more serious, they will need to consider whether it is necessary to draft such a particular domestic law. On the other hand, law-making organs of these certain countries in this dissertation do not update relative law to deal with problems about the dissimilation of organized crime, neither are the criminal laws against organized crime adjusted, nor are the criminal laws against cyber crime amended. These are reflected in two aspects, how to solve conflicts of criminal jurisdiction since the internet has changed the nature of joint crime theory that has not been reflected in the domestic criminal law of these countries. In view of the principal of a legally prescribed punishment for a specified crime having been followed worldwide, if the authorities of

a certain country want to take effective measures against organized crime in the internet age, it must adjust its relative domestic law.

7.2 Judiciary Obstacles

CTOC is known for having no frontier, but criminal justice is still defined in certain territory of one country. Apart from limitations of territory, gap and differences between various law systems are the other factors which lead to judiciary obstacles in combating cyber transnational organized crime. In the following section some judiciary obstacles will be discussed.

7.2.1 Judiciary Obstacles of Jurisdiction

Since the advent of the internet and the other ICTs, they have been developing with high speed. And the traditional transnational organized crimes in the real world have transferred to cyberspace with the aid of the internet and the other ICTs. Several years ago, smart-phones came into our life, with a smart-phone people can access to the internet anywhere as long as there are accessing internet signals. Mobile networks have further prompted the transfer of transnational organized crime into the cyberspace of mobile networks, which makes committing transnational organized crime much easier and convenient.TOC has been not restricted by the immovable IP address and immovable computer terminal, which means much fewer obstructions and a lower threshold for TOCGs.[232] In addition to the rapid and boundless character of the internet, each part of the whole process of one TOC may involve a great amount of countries.

[232] See Yu Zhigang, The Age of Informationalized Transnational Crime and Chinese Choice concerning The Council of Europe Convention on Cybercrime. Legal Forum, Issue 2, 2013.

Probably, this problem would lead to positive or negative conflicts of jurisdiction, but there is no concrete solution about how to solve these problems in domestic legislation, or regional and international conventions, especially in the aspect of a positive conflict of jurisdiction. For instance, in the 1990s of the last century the German Felix case revealed the positive conflict of jurisdiction, namely, the expansion of jurisdiction. Under this case the server which stored the child pornographic pictures was located in the controlling corporation of CompuServe in America, the users in Germany could browse or download these pictures, so the court of Germany held the opinion that German internet users could obtain these child pornographic pictures through the internet, further it held that this prejudicial act happened in Germany. On this basis, Germany had jurisdiction over this case, and then the so-called offender, Felix Somm, who was in charge of CompuServe in Germany was arrested by the relevant authorizes.[233] In 1998, Felix Somm was sentenced to 2 years imprisonment by the Munich district court of Germany.[234] It is not known whether America claimed jurisdiction over this case, but according to the territorial criminal jurisdiction America could have done so. Actually, this dissertation holds the opinion that the reasons why the Munich district court claimed that it had jurisdiction over this case, was based on the traditional rule of jurisdiction, were insufficient, even though the Munich district court held that German online users downloaded the child pornographic pictures in the territory of German, and based on this reason it executed its jurisdiction. In fact the server which stored the child pornographic pictures was located in the controlling corporation of CompuServe in America, and CompuServe's actions were only under the criminal jurisdiction of the USA. In this condition, we can make a supposition that America also claimed it had jurisdiction over this case. Inevitably, there would be a dispute about the jurisdiction over this case between Germany and America. Even though some articles or provisions of domestic law, regional or international

[233] Yang Caixia, The Enlightenment of International Anti-cybercrime Legislation to China—Taking the Council of Europe Convention on Cybercrime as the Focus, Present Day Law Science, Issue 3, 2008.
[234] Judgment of the Munich Court in the "CompuServe Case" (Somm Case), on-line news, Retrieved on 26.Oct.2013 from http://www.kuner.com/data/reg/somm.html.

conventions stipulate that the involved state parties should solve disputes of jurisdiction by means of negotiation, they are too ambiguous and vague, especially in the circumstances where is no particular principle dealing with jurisdiction of CTOC, the procedure of negotiation would waste time and the judiciary resources of the state parties involved. Obstacles of jurisdiction, positive and negative conflicts,[235] are a reflection of shortcomings of domestic law, and regional and international conventions concerning jurisdiction provisions. None of them fully considered the boundless and limitless features of the internet, finally resulting in judicial obstacles during the process of combating against cyber transnational organized crime.

7.2.2 Judiciary Obstacles of Investigating Cyber Transnational Organized Crime

Once a state party is involved, it establishes its jurisdiction over one CTOC, and an investigation will be launched over this case. In the condition of all state parties involved considering the case as a crime,[236] some judiciary difficulties are posed before investigators:

- A shortage of skilled investigators with ICTs.[237] Just as Robert W. Taylor, et al said the role of computers is growing rapidly in our society; law enforcement has lagged behind.[238] At present, not only is the role of computers growing rapidly, but so does the role of the internet and ICTs. The rapid growth of computers, the internet and ICTs also results in the boom of TOC in cyberspace. Usually criminals of TOCGs have corresponding ICTs for committing these crimes, so if the relevant authorities

[235] They will be analyzed in chapter 5 in detail.
[236] This is the pre-requisite if a involved state party intends to investigate one cyber transnational organized crime, in other words, only under the condition that all involved state parties consider this conduct as a crime, the state party which has established jurisdiction over the case has the right to carry out investigations with the judicial aid of the other state parties.
[237] Actually, this is a problem of recruitment in the law enforcement agencies, but lack of skilled investigators with ICTs would indirectly lead to judiciary obstacles when combating cyber transnational organized crimes.
[238] Robert W. Taylor, et al, (2006), *Digital crime and digital terrorism* (p.242), Pearson Education, Inc., Upper Saddle River, New Jersey.

of certain countries want to investigate these cyber transnational organized crimes, they must be equipped with skilled investigators with ICTs. As a matter of fact, due to the different levels of each country's legislation about cyber transnational organized crime and the limitations of its judiciary resources, the majority of countries are short of skilled investigators with ICTs. This problem has become a judiciary obstacle to combating transnational organized crime.[239]

- Lack of unified standards of how to investigate cyber transnational organized crime.[240] Because of the different levels of each country's legislation about organized crime and cybercrime, there is no unified standard concerning how investigators carry out cross-border investigations of cyber transnational organized crime. For example, since a crime scene in cyberspace is significantly different from a crime scene in the real world, investigators could depend on no standards of collecting, preserving, packing and transporting network evidence.

7.2.3 Judiciary Obstacles of Adjudicating on Cyber Transnational Organized Crime

The dissimilation of TOC by the internet also creates difficulties during the process of trials. One problem is which judiciary accusation is suitable for sentencing criminals of CTOC, and another problem is how to impose on the co-perpetrators criminal liability which can appropriately reflect their respective criminal responsibility. In the following section, two examples will be taken to illustrate these difficulties.

[239] Ibid.
[240] Ibid.

The first example, in judiciary practice it is a common phenomenon that criminals of TOCGs pass on hacker technologies. Under some conditions these hacker technologies are usually used by the other criminals to commit other relevant crimes. Then there are problems, should the conduct of imparting hacker technologies be considered as the crime of imparting criminal methods or the joint crime of the relevant crimes? In 2006 there was one case in the Henan province of China. The criminals were arrested because of carrying out the crime of imparting criminal methods.[241] It is questionable whether the suspects were charged with penalty responsibility for the crime of imparting criminal methods. On the one hand, this accusation requires imparting criminal methods to particular persons, but we do not know whether the criminal methods were imparted to particular persons in this case, and the fact is that in judiciary practice hacker technologies were usually imparted to unspecified people in cyberspace. On the other hand, there is also a need to analyze the nature of imparting hacker technologies under certain concrete cases. If the conduct of imparting hacker technologies were deemed to be a joint crime of a relevant type, should it be categorized to the extent of aiding conduct or abetingt (this will be analyzed in chapter 4).

The second example, from some online gambling cases that were used in chapter 2, the co-perpetrators of these cases developed online gambling software and programs, and they also rented overseas servers. Furthermore they provided these software and programs to the online gambling criminal groups for committing online transnational gambling.[242] It has become a judiciary obstacle of how to impose on these co-perpetrators criminal liability. Should these suspects who provide online gambling software and programs be prosecuted for being accessories to these online gambling cases, or should they be adjudicated according to another accusation? Furthermore, it

[241] Wang Minghao, Online Hacker School was dismantled by the Police of Xucang of Henan Province, On-line news, Retrieved on 27.Oct.2013 from http://www.people.com.cn/GB/paper464/16946/1488486.html.
[242] On-line news, Retrieved on 27.Oct.2013 from http://www.mps.gov.cn/n16/n1252/n1762/n2452/2461405.html.

would make the matter worse, if there are no relevant provisions in the criminal laws of those countries involved, these criminal conducts would escape from being punished.

8. Legislative Countermeasures Curbing Transnational Organized Crime in the Internet Era

There is a better way for duly updating and adjusting the existing national, regional and international laws to prevent cyber transnational organized crime, which can also tackle the corresponding judiciary obstacles. The proposals of how to update and adjust the existing national, regional and international law will be discussed in the following section.

8.1 Legislation for amending Legislative Absence and Loopholes

Legislation for amending legislative absence and loopholes will be proposed from the level of national criminal law, regional and international conventions to combat cyber transnational organized crime.

8.1.1 Legislation for amending Legislative Absence and Loopholes at National Level

In order to combat the increasingly serious cyber transnational organized crimes, each country needs to adopt new laws or amend its existing criminal laws.

Firstly, in the aspect of legislative forms, three types can be adopted, respectively, setting a new chapter to stipulate CTOC, stipulating CTOC in a different chapter of criminal code, and enacting particular criminal laws to combat CTOC. On account of different national conditions, individual countries can take a suitable legislative form to combat cyber transnational organized crime according to their own legal tradition.

Secondly, in the aspect of contents of legislation concerning cyber transnational organized crime, no matter which legislative form was adopted by an individual country, the contents of the legislation should include the following aspects:

- Criminal jurisdiction about CTOC. Since positive and negative criminal jurisdiction conflicts are increasing after the interaction and integration of TOC and cyber crime,[243] especially in the aspect of positive conflict. In order to avoid these problems, once an individual country claims criminal jurisdiction over one specific CTOC, a suitable criminal jurisdiction doctrine needs to be established at the level of national legislation, and it is better that this jurisdiction doctrine is generally recognized by the international society, such as a substantive damages connection principle (this principle will be analyzed in chapter 5).[244]

- New legal interests infringed by CTOC need to be specified in new provisions or under existing charges. Because of dissimilation of TOC by the internet, new types of interests need to be protected by domestic criminal law. For example, in China some criminal groups stole online game accounts or QQ (a instant messaging service) accounts in cyberspace, these accounts are intangible

[243] According to the cone diagram 1: the sum of involved countries' economic level, the bar diagram 3: the annual sum of cases involving developing countries and purely involved developed countries in chapter 2 and the over expansion of criminal jurisdiction concerning cybercrime in the relative clauses of the aforementioned countries' law, these positive conflicts are growing more numerous than before.

[244] This principle will be introduced in detail in chapter 5.

property, but actually the victims spent a great deal of money and time to upgrade their accounts, undoubtedly these accounts are the property of their owners. It is necessary to identify these intangible properties with virtual property and protect them by means of domestic criminal law. So new provisions need to be established to cover these new interests, or existing provisions should be amended to include them in the domestic criminal law. These would provide resolutions for judiciary obstacles when courts adjudicate CTOC.

8.1.2 Legislations for amending Legislative Absence and Loophole at Regional and International Level

At the regional and international level, two legislative forms can be adopted to combat CTOC. One is that of drafting a new convention to particularly combat CTOC. Another is amending related provisions under the existing conventions against cyber crime and TOC, such as the Council of Europe Convention on Cybercrime and the UNTOC. At present, it is much more difficult to draft new conventions at regional and international level to combat against CTOC than to amend the existing convention, because the former needs much more negotiation and compromise between different countries. Next we only discuss how to amend the existing conventions to combat CTOC, to be precise, how to amend and adjust the corresponding provisions of the Council of Europe Convention on Cybercrime and the UNTOC:

- Amending corresponding provisions of the Council of Europe Convention on Cybercrime. Firstly, the provision about jurisdiction. Article 22 of the Council of Europe Convention on Cybercrime concerns jurisdiction, but it only stipulates territorial criminal jurisdiction and personal criminal jurisdiction. The

protective criminal jurisdiction and universal criminal jurisdiction also need to be set under this article. In addition the territorial criminal jurisdiction needs to be amended. On the basis of territorial criminal jurisdiction substantive damages connection principle or other suitable standards of jurisdiction[245] should be established to solve the positive conflict of jurisdiction over cyber transnational organized crime. Secondly, in terms of the scope of crime category, four categories of cyber crime are stipulated in this convention, respectively, offences against confidentiality, integrity and availability of computer data and systems, computer-related offences, content-related offences and offences related to infringements of copyright and related rights.[246] Because CTOC also falls into the scope of cybercrime, just the four existing categories of cyber crime under this convention are insufficient to cope with the trend of interaction and integration between cyber crime and TOC in the era of the internet. Any traditional crimes that were committed by OCGs via the internet should be included in this cybercrime convention. So additional miscellaneous provision should be established, which stipulates the other traditional crimes committed by criminals via the internet which should be punished and fall in into the scope of cyber crime. Another provision also needs to be added under a suitable chapter, which set the guidelines for state parties to solve problems concerning the crimes of this convention committed by OCGs.

- Amendment of corresponding clauses of the UNTOC. At the time when the UNTOC was adopted and ratified 10 years ago, it did not fully anticipate the combination of transnational organized crime and cybercrime. Obviously, based on the increasing interaction and integration between these two types of crime in the internet age, some corresponding clauses need to be amended to cope with the evolution of transnational organized crime. Firstly, in terms of

[245] These standards of criminal jurisdiction will be analyzed in chapter 5.
[246] The Council of Europe Convention on Cybercrime.

jurisdiction, article 15 of this convention provides jurisdiction doctrines about TOC, but under this article only territorial criminal jurisdiction, personal criminal jurisdiction and protective criminal jurisdiction are included, in fact universal jurisdiction also needs to be stipulated within this article. It is also necessary to add one provision concerning how to solve positive and negative jurisdiction conflicts of transnational organized crime which occurs on the internet or related to ICTs. And for solving these problems, the available principles include a substantive damages connection principle or other more reasonable standards. Secondly, in terms of the scope of crime within this convention, article 2 can be considered as a miscellaneous provision about the scope of TOC. According to it, cyber transnational organized crime surely falls into the scope of transnational organized crime. However, the effect of combating cyber transnational organized crime would be much better if this convention added one provision that any transnational organized crimes committed by OCGs with ICTs should be criminalized and punished by state parties. Finally, those articles with the character of procedural law also need to be amended, such as the articles concerning confiscation and seizure related to ICTs, disposal of the confiscated proceeds of crime or property in cyberspace, mutual legal assistance concerning TOC which happened in cyberspace or is related to ICTs, joint investigations concerning CTOC, the standard of how to transfer criminal proceedings of CTOC and any other articles concerning combating CTOC.

The aforementioned are some proposals concerning the content of a cybercrime convention and how the UNTOC should be amended. In order to effectively operate against CTOC, it merits further research and negotiation on how to amend the corresponding provisions within these two documents.

8.2 Amendments of Procedural Law to Combat Cyber Transnational Organized Crime

Investigation and prosecution are also significant for combating CTOC, but in fact, evidence concerning CTOC is difficult to preserve and detect by law enforcement agencies; in contrast, these difficulties provide convenience for organized criminal groups to evade punishment. In addition, the loopholes of domestic procedural law aggravate this situation. Once an individual country affiliates to some regional or international conventions against cyber organized crime, for example, affiliating to the Council of Europe Convention on Cybercrime or the UNTOC, after the individual country becomes a state party of such conventions, it must amend and adjust its domestic procedural law concerning CTOC to abide by the principles of these conventions. The contents of domestic procedural law that need to be amended include confiscation and seizure related to ICTs, disposal of the confiscated proceeds of crime or property in cyberspace, mutual legal assistance concerning transnational organized crime which happened in cyberspace or is related to ICTs, joint investigations concerning CTOC, the standard of how to transfer criminal proceedings of CTOC, preservation of evidence and detection of CTOC.

Conclusion

This section introduces certain domestic, regional and international legislations against OC and cyber crime. However, the interaction and integration between TOC and cyber crime reveal the shortages when combating CTOC under these legislations: (1) even though the harm caused by cyber transnational organized crimes has grown in recent

years, particular domestic legislations have not been adopted to combat CTOC, nor have regional or international conventions been proposed to combat these crimes; (2) Provisions about joint crime under these legislations have been not amended after the structure of cyber organized criminal groups have been changed by the internet and ICTs;[247] (3) There are also no clear provisions to deal with conflicts of criminal jurisdiction about cyber transnational organized crime.

In order to solve these dilemmas: Firstly, at the level of domestic laws, in view of having recognized the above shortages, legislators should either amend corresponding provisions to solve these problems, or adopt particular laws or act to combat CTOC; At regional or international level, because there are overlaps between transnational organized crime, cybercrime and cyber transnational organized crime, actually, CTOC is the combination of cyber crime and transnational organized crime. At present, the existing efficient regional and international conventions against cyber crimes and transnational organized crimes include the Council of Europe Convention on Cybercrime, the United Nations Convention against Transnational Organized Crime and some protocols against particular transnational organized crimes. But in view of these conventions having manifested their insufficiencies when combating CTOC, there are two ways for improving the increasingly bad situation: One is drafting regional or international conventions or agreements to particularly combat CTOC, but it is still a question of whether it is the appropriate moment to take this way or not. Another way is taking low-cost and effective measures to prevent this type of crimes, which includes amending and adjusting corresponding provisions of the Convention on Cybercrime of Europe and the United Nations Convention on Transnational Organized Crime.[248] Furthermore, based on this work, related regional or international organizations should appeal for more countries to ratify and approve these conventions to combat CTOC.

[247] These changes will be analyzed in detail in chapter 4.
[248] The concrete measures that how to amend and adjust these conventions has been analyzed in the above part.

Section 2 Adjustments of Criminal Policy against Cyber Transnational Organized Crime Worldwide in the Internet Era

Criminal Policies mean various criminal countermeasures which are enacted or used by legislative institutions or judicial authorities according to their national conditions and crime situation. They are used to prevent crimes, and punish and correct offenders. Normally, the adjustments of criminal policy are the precursor of penal reform, so examining criminal policies against TOC in the context of the internet can provide us with resolutions and guidelines when solving problems resulting from CTOC. This part examines these policies at national, regional and international level.

1. Criminal Policies Against Organized Crime at National Level

In this part, some countries' criminal polices will be picked out as regional representatives, which include America, Italy, Austria, China and Australia.

1.1 Policies of the USA

Authorities of America have recognized that individual anti-organized crime measures cannot be successful when combating OC. Investigative efforts must be supported by quality intelligence gathering, collating, evaluating and dissemination to law enforcement agencies, prosecution, related government agencies, the private sector and public. Investigation of organized crime in turn has to be a co-operative effort by all

affected agencies. 4 points can be concluded concerning the adjustments of criminal policy of America against TOC:

- Increase the risks of involvement in OC by increasing OC law enforcement resources. [249]
- Increase the risks of involvement in OC by expanding the authority of OC law enforcement.[250]
- Reduce the economic lure of involvement in OC by making legitimate opportunities more readily available.[251]
- Decrease organized criminal opportunity.[252]

1.2 Policies of Italy

In Italy the majority of relevant anti-mafia measures were adopted as a result of particular events, such as homicides and attacks of criminal organizations against the state. For example, homicides of judges and policemen, the Capaci and via D'Amelio slaughters in which Giovanni Falcone and Paolo Borsellino were killed. This case was related to measures like the Decree-Act 306/1992 (so called "Falcone", dealing with trails and police action in the fight against the mafia). So the adjustments of criminal policy of Italy against transnational organized crime can be concluded as innovations concerning new criminal offences, investigatory powers and preventive measures, patrimonial preventive measures, checks relating to suspicious financial transactions and money laundering, the extensive use of collaborators of justice, special norms regarding mafia trials, judicial decisions concerning the interpretation of criminal and

[249] Howard Abadinsky, (1990), *Organized Crime* (Third Edition), Nelson-Hall Inc, p.481.
[250] Ibid.
[251] ibid
[252] ibid

procedural norms and regime of sanctions.[253] Since 2000, the law enforcement agencies have also taken some particular controlling and administrative measures in certain regions:[254] (1) Specific enforcement actions. In order to control and combat serious organized crimes in certain regions, Italian law enforcement agencies carried out some inter-departmental joint actions, by means of equipping extra staff and equipment to reinforce control of these regions; (2) Project of protecting witnesses. The Italian Interior Ministry implemented a project of protecting witnesses on 31.11.2000, which provided rigorous and carful protection for 1171 witnesses and their families who co-operated with law enforcement; (3) Dismissing regional Parliaments, The Italian government dismissed several regional parliaments due to Mafia penetration and effective influence; (4) Other public projects. In order to exclude Mafia' interference in public affairs, the Italian Interior Ministry also reinforced co-operation and information exchange with other public sectors; (5) Implementing regional action of "Italy-Albania" to prevent transnational organized crime. For example, on 13.12.2005, a joint action was carried out between these two countries to crack down on particular transnational organized crimes, such as enforced prostitution, drug dealing, weapon smuggling and illegal immigration.[255]

1.3 Policies of Austria

More than thirty years ago the phenomena of OC were denied in Austria, although actually it existed in Austria and was already proved by judicial practical experience.[256]

[253] Antonio La Spina, The Paradox of Effectiveness: Growth, Institutionalization and Evaluation of Anti-Mafia Policies in Italy, In Cyrille Fijnaut and Letizia Paoli (ed.) (2004), *Organized Crime in Europe: Concepts Patterns and Control Policies in the European Union and Beyond*, Springer, p.643-644.

[254] Gu Wenling, Research on European Organized Crime, East China University of Politics and Law, issued on 18.April.203.

[255] Online news, retrieved on 10.Sep.2014 from http://news.qq.com/a/20051214/000497.htm.

[256] Maximilian Edelbacer, Organized Crime: An Austrian Perspective, I N S. Einstein and M. Amir (ed.) (1999), Organized Crime: Uncertainties and Dilemmas, the Office of International Criminal Justice, the University of Illionis at Chicago, p.254.

The adjustments of criminal policy of Austria against organized crime OC can be generalized as adjustments of legislation against organized crime. At present, that perception has changed. The terms about organized crime set out in the Security Police Act, article 164,165, 278, 278a 278b and 279 of the Criminal Code of Austria are used to combat organized crime, and the European Community measures against money laundering were introduced into the banking law and in the penal code in 1994.[257] In the aspect of regional or international cooperation against international organized crime, on 01.March.2005 one agreement, Cooperation in Combating International Organized Crime, was signed between the Austrian Interior Ministry and Serbian Interior Ministry. This agreement focuses on combating international illicit trafficking of narcotics and international terrorism.[258]

1.4 Policies of China

The adjustments of criminal policy of China against organized crime can be categorized into countermeasures and preventive measures.

In the respect of countermeasures, the Criminal Code of China focuses on punishment of organizing, leading, taking part in criminal organizations with a character of an underground gang, entering the territory of China to develop OCGs, and harboring or conniving with criminal organizations with the character of an underground gang. In fact this Chinese law enforcement often launched particular activities to combat OC nationwide or co-operated with its neighbors to counter specific organized crimes, such

[257] Ibid.
[258] On-line resources, retrieved on 10.Sep.2014 from http://www.ris.bka.gv.at/Bundesrecht/.

as co-operating with Burma, Vietnam, Thailand and Malaysia to counter drug trafficking and telecommunication fraud.[259]

In the aspect of preventive measures, in order to control OC, the authorities of China take the "enhancing comprehensive treatment of social security, combining the counter-measures and preventive measures, and prevention first" as guiding principles from macro-scale and criminal policy of combination of punishment with leniency against organized crime. Under these guidelines some concrete preventive measures are taken by law enforcements, including legislative prevention which is reflected by the original local regulations of Shenzhen city of China and judicial prevention. The judicial prevention can be generalized from the following aspects:[260]

- Emphasizing the strategy utilization, law enforcement agencies of China do their utmost to nip organized crime in the bud.
- Reinforcing the fight against corruption to eradicate the protective umbrella of organized crime.
- Spreading propaganda and mobilizing the masses to combat organized crime. The general public often provides law enforcement agencies with important clues about organized crime.
- Reinforcing international co-operation against organized crime, since transnational organized crime is becoming much more serious with the help of ICTs.

1.5 Policies of Australia

[259] Lu Jianping eds. *Comparative Study of Organized Crime*, Law Press • China, 2004, P.94-107.
[260] Ibid.

In order to counter and prevent organized crime, Australia has also adjusted its criminal policy. One prominent adjustment of Australian criminal policy is the establishment of a National Crime Authority on 1 July 1984. The National Crime Authority Act 1984 conferred on the NCA a great number of coercive powers, such as the ability to compel people to produce documents and to appear before the Authority to give sworn evidence. NCA also has a national as well as a multi-jurisdictional focus and can investigate offences against Federal as well as State and Territory laws. It can also use facilities such as telephone interception and listening devices. Usually, these investigative tools are only available after a judicial warrant has been obtained under the relevant Federal and State or Territory legislation. In judicial practice, law enforces of Australia often consider a number of factors to counter OC. These factors include political commitment, adequate powers, funding, public support, co-operation, partnerships, co-ordination, that jurisdictional boundaries must be broken down, and complementary legislation.[261] However in the federal NCA, at the state level, almost all state police offices have their own criminal intelligence agency to counter organized crime.[262]

2. **Regional Criminal Policies against Organized Crime**

In view of the European Union being more unified than the other regional organizations, this part only briefly introduces the general policy of the European Union on organized crime.

In the late 1970s the Member States of the European Union began to exchange information on terrorism and later on, on organized crime in the so-called TREVI

[261] John Broome, Organized Crime: An Australian Perspective, In *Organized Crime: A World Perspective*, Third International Police Executive Symposium, Kanagawa University, Yokohama, Japan Nov 28-Dec 1, 1996, The Society of Law, University of Kanagawa, Vol.31, No. 3, 1997, p.280.

[262] Lu Jianping eds. *Comparative Study of Organized Crime*, Law Press • China, 2004, P.114.

working groups.[263] The fight against OC, especially drug and arms trafficking was an important factor when drawing up the Schengen Application Convention. The Council Directive of 10 June 1991 on the prevention of the use of the financial system for the purpose of money laundering was also intended to counter organized crime. On Sept 1992 the Ministers of Justice and Interior established an Ad Hoc Working Group on International Organized Crime and assigned it the task of investigating ways of intensifying the joint efforts of the Member States against organized crime, and two reports were compiled by the working group in 1993.[264] The first report emphasized the importance of co-operation between customs authorities and a few lines were also devoted to the preventive approach to organized crime. The second report put forward proposals to start systematically collecting information on organized crime in the European Union, improve legislation in the member states in a number of areas, and use the "administrative measures likely to hinder the development of international organized crime".[265] In 1996 when Ireland held the Presidency of the European Union, it made a decision at the Dublin Summit on 13 and 14 December 1996 to set up a High Level Group of Officials, who were to draw up a "comprehensive action plan" before April 1997 for combating organized crime. This comprehensive plan consisted of a draft of measures to forcefully promote co-operation between the Member States in criminal matters. Following this preventive section of the plan, on Dec 1998 the European Council adopted a resolution "on the prevention of organized crime with reference to the establishment of a comprehensive strategy for combating it". In May 2000, as a result of the 1998 resolution, a report was published in the Official Journal: The Prevention and Control of Organized Crime, a European Union Strategy for the Beginning of the New Millennium. The strategy set down under this policy document was embodied in 39 recommendations, which build on the measures that have been announced in all previously mentioned plans, including the action plan to combat

[263] Cyrille Fijnaut and Letizia Paoli, The Initiatives of the European Union and the Council of Europe, In Cyrille Fijnaut and Letizia Paoli (ed.) (2004), *Organized Crime in Europe: Concepts Patterns and Control Policies in the European Union and Beyond*, Springer, p.633.
[264] Ibid.
[265] Ibid, p.634.

organized crime and the Tampere program. A symposium was organized by the Dutch Presidency of the European Union on 10 and 11 June 2004 in The Hague on the development of a new strategic concept. At the meeting the issues discussed included establishing the key priorities of the policy of the European Union, ways of increasing insight into organized crime and improving the actual use of existing instruments within the European Union and new approaches in the fight against organized crime.[266]

In recent years, the Council of Europe also realized cyber organized crime is becoming much more serious than before, since the Council of Europe's Convention on Cyber Crime was adopted in Budapest in Nov 2001, a range of other measures have been implemented by Member States' governments of the European Union.[267] These measures can be considered as the adjustments of criminal policy against cyber crime in Europe.[268]

- International standards and co-operation. Actually, the Council of Europe's Convention on Cyber Crime serves as a global standard, which requires a pre-condition for criminal justice action against cyber crime that the conduct to be investigated, prosecuted, and adjudicated is defined as a criminal offense, and it farther asks that the substantive and procedural legislation among the Member States has to be compatible and reciprocal.[269]

- Cyber crime reporting. The reporting systems should be established, which provide the public and criminal justice authorities with the necessary information to detect cyber crime and whether apparently minor fraud schemes are part of a major

[266] Cyrille Fijnaut and Letizia Paoli, The Initiatives of the European Union and the Council of Europe, In Cyrille Fijnaut and Letizia Paoli (ed.) (2004), *Organized Crime in Europe: Concepts Patterns and Control Policies in the European Union and Beyond*, Springer, p.633-637.
[267] Alexander Seger, Cyber Crime and Economic Crime, In Maximillian Edelbacher, Peter Kratcoski and Michael Theil (ed) (2012), *Financial Crimes: A Threat to Global Security* , CRC Press, p.137.
[268] Alexander Seger, Cyber Crime and Economic Crime, In Maximillian Edelbacher, Peter Kratcoski and Michael Theil (ed) (2012), *Financial Crimes: A Threat to Global Security* , CRC Press, p.138-142.
[269] Its legal bases are the Budapest Convention, the recommendations of the Financial Action Task Force (FATF), the Council of Europe Convention on laundering, search, seizure, and Confiscation of Proceeds from Crime and on the Financing of Terrorism.

criminal operation, and in the European Union, an Internet Crime Reporting Online System (I-CROS) is being established at Europol.[270]

- Due diligence of registries and registrars of domains. In many cases, domain name registries and registrars fail to exercise due diligence results in the operation of botnets and other cyber crimes.[271]

- Specialized units and inter-agency co-operation. The Member States of European Union have also begun to create specialized prosecution and high-tech crime police services responsible for investigating and prosecuting cyber crime.[272]

- Public and private co-operation. Co-operation and information exchange between public and private sectors can achieve a major impact, such as information sharing and analysis centers (ISACs) for the financial sector in the U.S., Netherlands and other countries. To further strengthen cooperation among law enforcement agencies and internet service providers, in 2008 the Council of European developed guidelines for law enforcement and ISP co-operation in the investigation of cyber crime.[273]

- Training. Since most transnational organized crime has involved the internet and thus yielded electronic evidence, this asks law enforcement officers, prosecutors and judges to get basic knowledge of cyber crime and electronics. The training concerning this knowledge is necessary. The European Cyber Crime Training and Education Groups (ECTEG) have been responsible for this training for several years.[274]

---

[270] Alexander Seger, Cyber Crime and Economic Crime, In Maximillian Edelbacher, Peter Kratcoski and Michael Theil (ed) (2012), *Financial Crimes: A Threat to Global Security* , CRC Press, p.139.

[271] Its legal basis is the Law Enforcement Recommended Amendments to ICANN's Registrar Accreditation Agreement (RAA) and Due Diligence Recommendations.

[272] Alexander Seger, Cyber Crime and Economic Crime, In Maximillian Edelbacher, Peter Kratcoski and Michael Theil (ed) (2012), *Financial Crimes: A Threat to Global Security* , CRC Press, p.141.

[273] The Council of Europe in 2008 developed guidelines for law enforcement and ISP cooperation in the investigation of cyber crime.

[274] The Council of Europe in 2009 adopted a "concept for cyber crime training for judges and prosecutors" to incorporate such training in domestic training programs.

- Efficient international cooperation. Cyber transnational organized crime is a difficult problem involving many countries instead of involving only one country, so it is necessary to strengthen international co-operation to counter cyber crime. For example, the Council of Europe's Convention on Cyber Crime provides its Member States with guidelines concerning the establishment of co-operation on combating cyber crime.[275]

3. **International Criminal Policies against Transnational Organized Crime**

The work of the United Nations in strengthening international co-operation against organized crime dates back more than thirty years. Apart from the UN Convention against organized crime and some supplementary protocols against specific organized crime, related international organizations also adjusted criminal policies to effectively combat TOC..

Since 1975, there have been various United Nations' reports and resolutions concerning OC. In 1975 the Fifth United Nations Congress on Crime Prevention examined the topic devoted to the "Changes in Forms and Dimensions of Criminality- Transnational and National" under its agenda item 4. It focused on crime as business at the national and transnational levels: organized crime, white-collar crime and corruption. In 1980 the Sixth United Nations Congress on Crime Prevention, under its agenda item 5 entitled "Crime and the Abuse of Power: Offences and Offenders beyond the Reach of the Law", added new elements to the international perception of organized crime. The issue was considered farther by the Seventh United Nations Congress on Crime Prevention in

[275] Its legal bases are the Budapest Convention, the recommendations of the FATF, Warsaw Convention, the Council of Europe Convention on laundering, search, seizure, and Confiscation of Proceeds from Crime and on the Financing of Terrorism and Interpol's I-24/7 global communication system and its National Central Reference Points (NRCP) network of designated investigators in national computer crime units in more than 120 countries.

1985 under topic Ⅰ "New dimensions of Criminality and crime prevention in the context of development: challenges for the future." In 1988 a plenipotentiary conference, held in Vienna, adopted the United Nations Convention against Illicit Trafficking in Narcotic Drugs and Psychotropic Substances. In 1990 the Eighth United Nations Congress on Crime Prevention examined the problems of organized transnational crime in the light of new historic developments within the framework of its topic Ⅲ "Effective national and international action against organized crime and terrorist criminal activities." In 1992 the Commission on Crime Prevention and Criminal Justice was established and held its first session. On its recommendation the Economic and Social Council adopted resolution 1992/22, by which the Economic and Social Council determined that one of the priority themes that should guide the work of the Commission and the United Nations Crime Prevention and Criminal Justice Programme would be "national and transnational crime, organized crime, economic crime, including money laundering, and the role of criminal law in the protection of the environment." At the first session of the Commission on Crime Prevention and Criminal Justice, it adopted resolution 1/2 on "control of the proceeds of crime," by which it requested the Secretary-General to examine the possibility of co-ordinating efforts made at the multilateral level against the laundering of proceeds of crime and related offences, and to propose means for technical assistance for Member States in drafting legislation, training of law enforcement personnel, developing regional, sub-regional and bilateral cooperation and in providing advice. In 1994, The Naples Political Declaration and Global Action Plan against Organized Transnational Crime was adopted on the World Ministerial Conference on Organized Transnational Crime. It emphasized the need and urgency for global action against Organized Transnational Crime, focusing on the structural characteristics of criminal organizations. In 1995, the Buenos Aires Declaration on Prevention and Control of Organized Transnational Crime was adopted by a Latin American Ministerial Workshop which was hosted by the Government of Argentina in Buenos Aires. In 1996, the General Assembly adopted the United Nations Declaration on Crime and Public Security and the United Nations Declaration against

Corruption and Bribery in International Commercial Transactions. In 1997 the General Assembly adopted resolution 52/85, by which it decided to establish an inter-sessional inter-governmental expert group of the commission to elaborate a preliminary draft of an international convention against organized transnational crime. The Government of Poland had offered to host a meeting of this expert group at Warsaw in Feb 1998. As a result of this, the United Nations Convention against Transnational Organized Crime was adopted by the 55th General Assembly in 2000.[276]

At present, Cybercrime is a fast-growing area of crime. More and more criminals are exploiting the speed, convenience and anonymity of the Internet to commit a diverse range of criminal activities that know no borders, either physical or virtual.[277] Once cyber crime is committed by OCGs it involves more than one country, and in this condition, such cyber crime has become TOC. In other words, the harm caused by cyber crime that takes place in the borderless cyberspace is aggravated by the increasing involvement of OCGs. At the international level, the United Nations Office on Drugs and Crime (UNODC) promotes long-term and sustainable capacity building in the fight against cyber crime through supporting national structures and action. Specifically, UNODC uses its specialized expertise on criminal justice systems to provide technical assistance in capacity building, prevention and awareness raising, international co-operation, data collection, research and analysis on cyber crime.[278] These works of UNODC are the international countermeasures against cyber crime. It is obvious that the international community has paid attention to the combination of transnational organized crime and cyber crime, and some related international organizations have begun to adjust their policy to counter and control them.

[276] M.Cherif Bassiouni and Eduardo Vetere, (1998), Towards Understanding Organized Crime and Its Transnational Manifestations, M.Cherif Bassiouni and Eduardo Vetere, (eds), In *Organized Crime: A Compilation of U.N. Documents 1975-1998*, Transnational Publishers, Inc.

[277] On-line report, retrieved on 27. 06. 2015 from http://www.interpol.com/.

[278] On-line article (2013). Retrieved on 19.Sept. 2013 from http://www.unodc.org/unodc/en/organized-crime/emerging-crimes.html.

Conclusion

This section discusses adjustments of criminal policy against CTOC in the internet era, since the adjustments of criminal polices can indicate directions of legislations for combating CTOC. By means of the work of this section, i.e., examining the adjustments of Criminal Policy adjustments of criminal policy against CTOC in the internet era, we can know which aspects of criminal policies against cyber transnational organized crime are more necessary and urgent at present. During the process of adjusting the criminal policies against CTOC and cyber crime, we must always notice that the natures of CTOC and cyber crime are changing, which are indicated by the following aspects: (1) In the past, cybercrime was committed mainly by individuals or small groups. Today, we are seeing criminal organizations working with criminally minded technology professionals to commit cybercrime, often to fund other illegal activities. Highly complex, these cybercriminal networks bring together individuals from across the globe in real time to commit crimes on an unprecedented scale; [279] (2) Criminal organizations turn increasingly to the internet to facilitate their activities and maximize their profit in the shortest time. On the one hand, the crimes themselves are not necessarily new – such as theft, fraud, illegal gambling, sale of fake medicines – but they are evolving in line with the opportunities presented online and therefore becoming more widespread and damaging. On the other hand, these OCGs are also beginning to become involved in crimes related to ICTs.

[279] Ibid.

Chapter 4 Dilemmas of Joint Crime Theory and Corresponding Resolutions under Cyber Transnational Organized Crime

The previous chapter investigated the criminal legislations and adjustments of criminal policy against OC, TOC and cyber crime, and analyzed legislative loopholes and weaknesses when dealing with the trend of interaction and integration between TOC and cyber crime, namely coping with CTOC. This chapter analyzes the dilemmas of joint crime theory under CTOC. These dilemmas and obstacles result from the combination of transnational organized crime and cyber crime. Accordingly, they have already led to some corresponding problems that traditional criminal theories, criminal legislations and judicial rules are not easy to apply to in juridical practice.

Section 1 Evolution of the structure of Joint Crime under Cyber Transnational Organized Crime

It is widely acknowledged that the internet and ICTs are creating a new era for human beings. On the one hand, the internet and ICTs are closely connected with the real world. On the other hand, their natures significantly differentiate themselves from the real world as they create completely new platforms where human can carry out almost all kinds of activities. The virtual nature of cyberspace leads to difficulties in applying traditional criminal theory to CTOC. For example, both the aidant act[280] and organization conduct under joint crime theory have been changed by the character of the internet, and accordingly, they should be re-evaluated by criminal theory.[281] Based on

[280] the aidant act is a type of criminal behaviour, which is conducted by certain accessary offenders under the joint crime, these accessary offenders help the principle offenders to complete the whole crime.
[281] This will be analyzed in detail in the following text.

the work of chapter 3, in which the loopholes and absences of joint crime theory about CTOC have been briefly discussed, next these issues will be analyzed in detail.

1. Structure of Traditional Organized Crimes

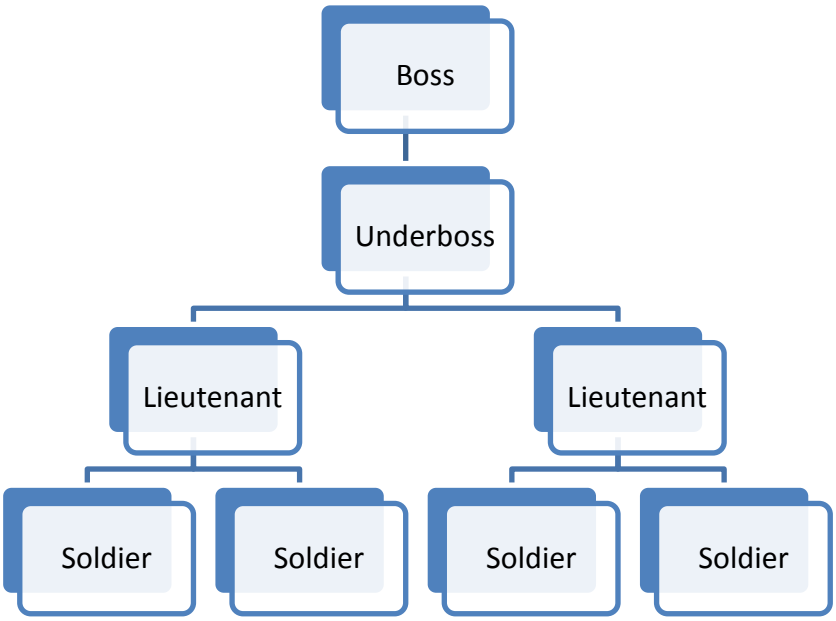
In order to complete the whole process of crimes and achieve the goals of crimes, mutual co-operation between the members of OCGs is the original incentive which further promotes the establishment of OCGs. The basic reason is that one single offender cannot solve all the problems during the process of committing crimes, and it is necessary to complete the goals of OCGs by means of teamwork.[282] Therefore, generally speaking, traditional organized criminal groups are often provided with a rigorous structure, which further distinguishes them from simple joint crimes. The basic models of traditional organized criminal groups can be concluded as follows:

1.1 Pyramid Structure

Pyramid structure is one common model of traditional organized criminal groups, such as the Italian Mafia and Camorra, which can be well indicated by figure 1. The members of this type of traditional organized criminal group are generally intertwined with each other via family origins and blood.[283] This clan hierarchical system stemmed from Italian Sicily and Naples, where the Mafia and Camorra were secret criminal societies that were established on the basis of local farmers who strived for survival. Later they spread over the other regions of world, especially in the USA.

[282] See Sun Yinhan, Research on Organized Political Consciousnesses of Organizational Praxiology, cited in Wang Li, eds, *Monographic Study on Organized Crime*, Issued in 2007, people's publishing house, p.98.
[283] See, Richard Gambino, My Blood: the Dilemma of the Italian-Americans, Cited in Howard Abadinsky, Organized Crime, Third Edition, Nelson-Hall Publishers/Chicago, P.9.

Figure 1: Pyramid structure



The common characteristics of the pyramid structure of traditional organized crimes can be concluded as:

- Complicated hierarchical structure. Mafia-type of OCGs is usually provided with a rigorous pyramid structure of clan hierarchical system. As illustrated in the figure 1, this type is commonly with two or three, or even more classes, every class is provided with a position for its own boss, whose power is inherent, and it does not depend on the person who takes the position at a particular time.[284]

- Clear division of labor. There are clear divisions of labor in a pyramid structure of traditional organized crime. In order to maintain the groups' illegal activities, the members with different qualities and techniques are usually settled in different positions. An assignment often involves commanders and enforcers. The commanders are often the boss of the upper classes, the enforcers directly or indirectly accept assignments from the upper boss, and implement it by themselves or assign it to other lower members. If the group is sophisticated enough, it may also have positions for a fixer, money mover and intelligence analyst. The fixer excels in

[284] Howard Abadinsky, Organized Crime, Third Edition, Nelson-Hall Publishers/Chicago, P.9

developing contacts with criminal justice and/or political officials and, when appropriate, uses corrupt methods. The money-mover is an expert at "laundering" illicitly obtained money, disguising its origin through a string of transactions and investing it in legitimate enterprises.[285] The intelligence analysts provide the groups with all kinds of information, and analyze information for the groups' illegal activities.

- There are blood and marriage-kin relationships between members, especially through the paternal line to extend and broaden the power of the group.[286]

- Such groups are equipped with rigorous discipline and rules. By means of rigorous discipline and rules it constrains the behavior of its members. Such as:[287] (1) Always show rispetto to those who can command it; (2) Report any failure to show rispetto to one's immediate superiorly; (3) Violence must be used, even if only of a limited type, to ensure rispetto; (4) Never ask for surnames; (5) Never resort to violence in a dispute with a member or associate of another family; (6) Do not use the telephone except to arrange for a meeting place, preferably in code, from which you will then travel to a safe place to discuss business; (7) Avoid mentioning specifics when discussing business beyond those absolutely necessary for understanding; (8) Keep your mouth shut; (9) Do not ask unnecessary questions, the amount of information given to you is all you need to carry out your job; (10) If your patron arranges for two parties to work together, he assumes responsibilities for arbitrating any disputes between the parties; (11) The boss can unilaterally direct violence, including murder, against any member of his family, but he cannot engage in murder-for-hire, that is, make a profit from murder; (12) The boss cannot use violence against a member or close associate of another family without prior consultation with that family's boss.

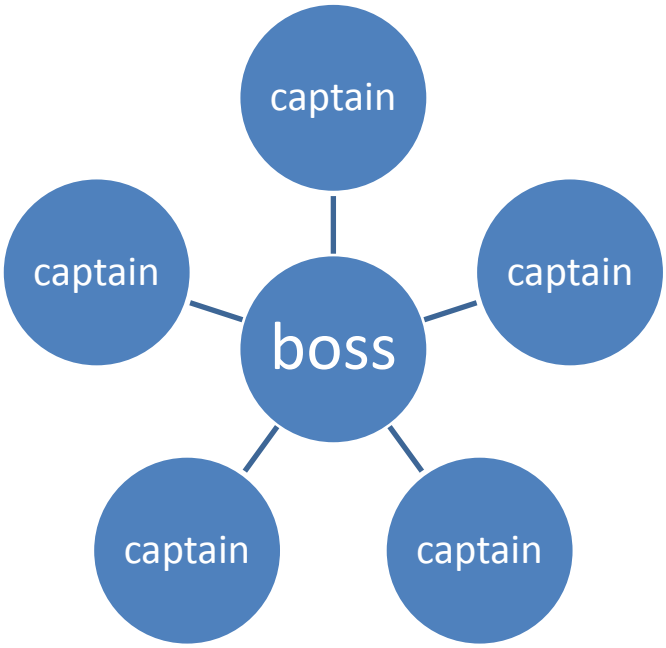
[285] Ibid.
[286] ibid
[287] Ibid. p.41.

1.2 Structure of Hub-and-Spoke Model

The structure of the Hub-and Spoke model is another common type of traditional organized crime, as shown in figure 2. Traditional Italian-Americans OCGs fall into the scope of this model. Obviously, the main differences between this type and the pyramid structure are that the relationship between the members of the former type is not maintained by blood and marriage-kin. As figure 2 showing, the core of Hub-and-Spoke model is the Hub, i.e., the boss of traditional organized criminal groups, accordingly, the terminals of the spoke are the captains. Furthermore, each captain and his/her sub-members further constitute many small Hub-and-Spoke models, but there are no direct relationships between these members and the uppermost boss.[288] These bigger and smaller Hub-and Spoke models are "fixed" together via "spokes" and generate all kinds of contact of common criminal intentions to promote the operation and illegal activities of these groups.

Figure 2: Structure of Hub-and Spoke model

[288]See, Richard Gambino, My Blood: the Dilemma of the Italian-Americans, Cited in Howard Abadinsky, Organized Crime, Third Edition, Nelson-Hall Publishers/Chicago, p.30.



2. Evolution of Cyber Organized Criminal Groups

Along with the widespread use of the internet worldwide, it is unnecessary that dissemination of information between individuals still follows the top-down processing, by means of the internet and the other ICTs people can directly or indirectly communicate with each other. Accordingly, the approaches of information communication without hierarchy greatly stimulate and promote the evolution of large and small traditional organized criminal groups. Generally speaking, the main models of organized criminal groups in the internet age are as follows.

2.1 Network Structure

Network structure of OCG, as figure 3 shows, is one manifestation of the evolution of traditional organized criminal groups, which can be revealed by a typical case of OC.

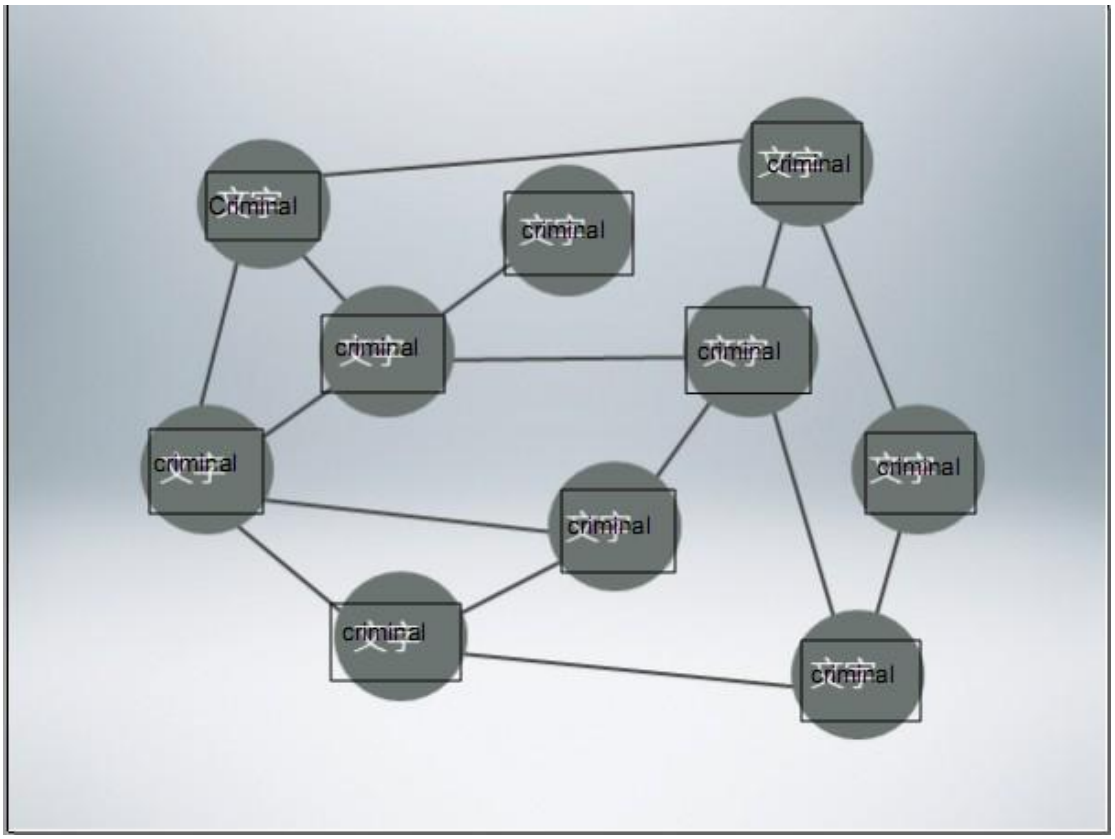
For example, in November of 2007 the police of Hefei City of Anhui Province of China uncovered the "6.26" drug dealing case, this drug dealing organized criminal group was composed of 14 smaller groups, the members used the internet or other information communication techniques, and sometimes they purchased drugs together but sold them separately, at another times they exchanged drugs to support each other, they set selling prices by negotiation, and almost controlled the supply channel and selling market of new types of drugs in Hefei; the members even shared the name lists of drug users, and they communicated online to regulate the supply and demand of drugs. Finally, a typical intertwined network structure of OCG was established by means of the internet and other ICTs.[289]

The members of OCGs use the internet and other ICTs to exchange criminal experiences and information, and even carry out criminal techniques training, and imparting criminal knowledge and skills. It can be said that the convenient and fast ICTs provide conditions and chances for the evolution of traditional organized criminal groups from traditional structures into a network structure. Evidently the character of having no obvious central leading organs or command center distinguishes this network structure from traditional structures. Unlike traditional pyramid structure and Hub-and-Spoke structures, network structure has no obvious classes existing in the whole OCGs; sometimes there are relatively loose classes around one or some nodes in the whole network of OCGs. However, network structure has no power center, it is possible that there are some so-called leaders in the whole criminal network, but decision-making authority is decentralized and transferred to the other members, the smaller groups and single member are the nodes of whole criminal networks. The members contact each other at the lateral direction, and they exert their initiative and autonomy at their corresponding position to maintain the operation of OCG. Commonly

[289] On-line news, retrieved on 16.september.2014 from http://www.chinanews.com/gn/news/2007/12-25/1114636.shtml

there are some cohesive forces, common criminal goals and ideology, existing among the members, as a bond which provides the members with specific goals when they make decision or commit crimes, so it is unnecessary that the criminal network must be provided with hierarchical and vertical leading power. The most important advantage for a complicated network structure of OCG is that its functions and operation cannot be obviously influenced, even if one of its nodes is destroyed or removed.[290] Of course, such an advantage also causes the network structure OCGs to be difficult to combat and destroy.

Figure 3: network structure



2.2 Structure of Aggregate Ray

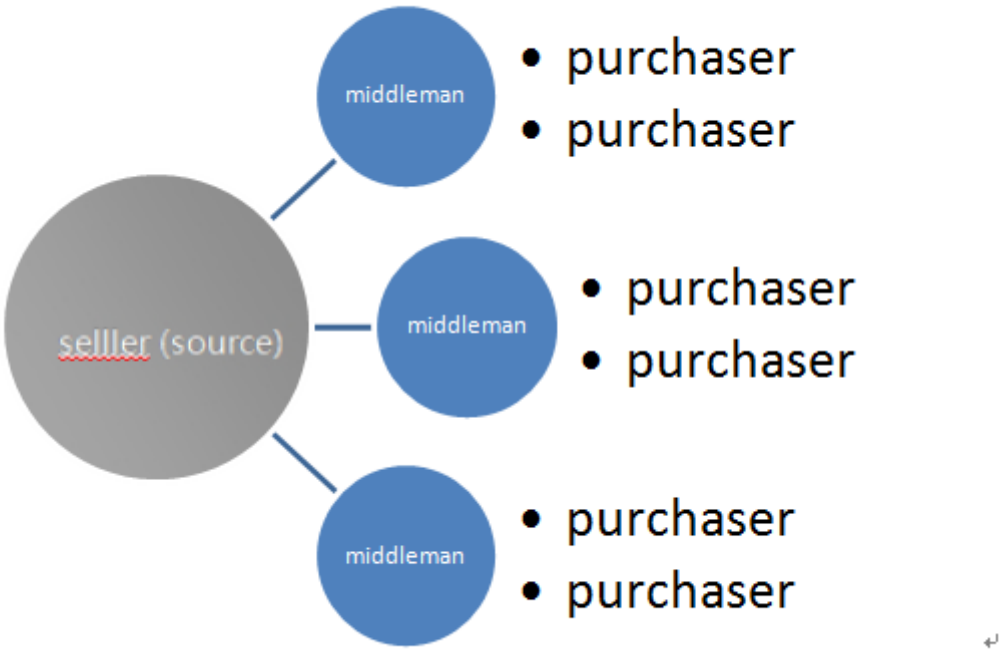
[290] On-line news, retrieved on 16.september.2014 from http://www.docin.com/p-771707862.html

The structure of aggregate ray is another evolution of traditional organized criminal groups, which is illustrated by figure 4. For instance, a typical case can reveal this structure. In 2012 China and the USA successfully uncovered a transnational organized crime network of smuggling arms, almost all illegal conduct of this case was carried out online; four basic segments are included in this case, i.e., seller (the source of the arms), middlemen in the USA, middlemen in China and purchasers in China. Middlemen Lin and Li established an online organized criminal group to smuggle and deal arms for the seller, Joseph.Dibosai, who was a staff sergeant of the United States National Guard. Lin and Li indirectly posted arms to the purchasers by the middlemen in China.[291] The criminal chain of this case ran across two countries, China and USA, the seller (source) and American middlemen were in the territory of the USA, and the Chinese middlemen and purchasers were in China, the criminals also used false identities, addresses and contact information via the internet to make deals.

Even though there is a similarity between the extrinsic feature of the Structure of aggregate ray and structure of the Hub-and Spoke model, actually their nature is different. Under the case that has just been discussed in this part, the American seller is the source of the whole case, but he is not the central power of this OCG. The seller, the middlemen and the Chinese purchasers do not know and meet each other in real life. Actually, there was no central power or leaders in this type of OCGs. The OCGs with a structure of the aggregate type takes the cyberspace/internet as the platform to commit crimes. In contrast, the OCGs with a structure of the Hub-and Spoke model commit crimes in the real world. The boss is the central power of the whole group, the captains who are under the boss, and the sub-members under the captains know each other, they co-ordinate with each other to commit crimes.

Figure 4: the structure of aggregate ray

[291] On-line news, retrieved on 16.september.2014 from http://www.mps.gov.cn/n16/n1252/n1687/n2272/3414264.html



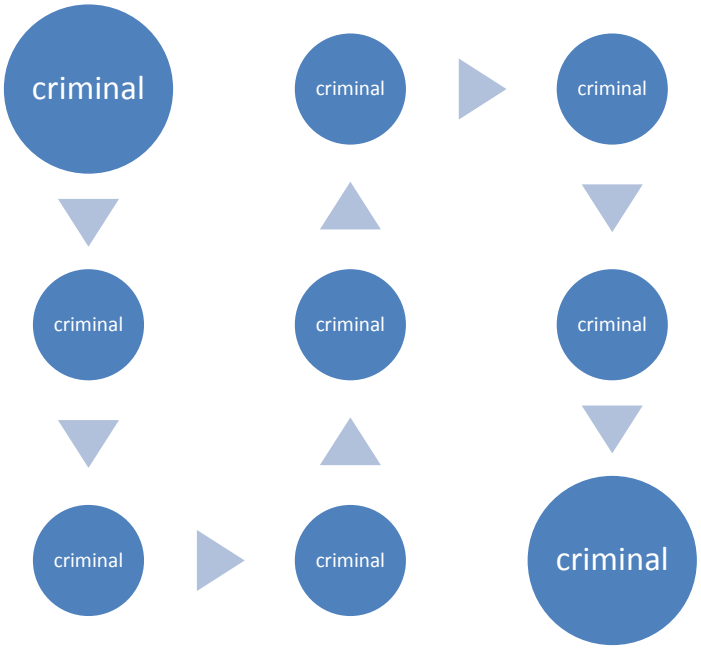
2.3 Chain Structure

Chain structure, as figure 5 shows, is also another manifestation of the evolution of OCGs. The chain structure is well revealed by online stealing information-fraud cases. For example, Beijing police uncovered a case in July of 2010, in which the members of a criminal group programmed, sold and used hacker-technologies, such as virus programs. With these hacker-technologies the members stole passwords of online users' QQ accounts, and further they used this stolen personal information to commit online fraud. In this case, the division of labor is precise; there are several segments existing in the whole chain of the criminal activities, including programmers of Trojan horse code, senior selling agents, second-level selling agents and the members who are in charge of the turnover and withdrawal of criminal capital.[292] There should be at least three nodes

[292] On-line news, retrieved on 16.september.2014 from http://www.mps.gov.cn/n16/n1252/n1762/n2452/2580402.html.

in the OCGs with a chain structure. At each node there are one or more criminals who are in charge of their own responsibilities in the whole criminal chain. They communicate and exchange criminal information to commit crimes.

Figure 5: Chain structure



Section 2 Dilemmas and Corresponding Solutions of Joint Crime Theory under Cyber Transnational Organized Crime

Under the influence of the internet and the internet-related ICTs, some dilemmas of joint crime theory are merging along with the trend of interaction and integration between TOC and cyber crime. The structures of CTOC mainly include Network structure, Network structure and Chain structure. Actually these three types reveal a trend, De-hierarchy (non-hierarchical), of CTOC. De-hierarchy means, compared with the pyramid structure and the structure of the Hub-and Spoke model of traditional organized criminal groups, there is no rigid central power and central leaders in CTOC;

the level of power and division of labor have been relatively weakened by the internet and the internet-related ICTs. The members of cyber transnational organized criminal groups rarely contact each other in normal social life, and never see each other. Accordingly, there are no strict regulations or rules to restrain the behavior of members, the common criminal goals and criminal intent are the only cohesive force of cyber transnational organized criminal groups.

1. Dissimilation of Category of Joint Offenders by De-hierarchy

According to the joint crime theory, there are two criteria about the category of joint offenders worldwide: (1) In accordance with the criterion of division of labor, the joint offenders are categorized into organizing offenders, perpetrators, abettors and accessories (aider); (2) according to the criterion of the function of joint offenders, they are classified as principals and accessories.[293] The Chinese Criminal Code takes an eclectic criterion, which is mainly based on the criterion of division of labor, and takes the criterion of function of joint offenders as a supplement. In accordance with this criterion, joint offenders are categorized as principals, accessories, abettors and coerced offenders.[294]

In line with traditional criminal theory, the act of joint offenders can be categorized as the act of perpetrating, organizational conduct, act of aiding and abetting . But at present the stable internal structure of joint offenders in a real world are being changed by the trend of interaction and integration between TOC and cyber crime., and the original

[293] See Wang Li eds, *Monographic Study on Organized Crimes*, People's Publishing House, issued in 2007, p.97.
[294] Ibid.

boundary between the act of perpetrating, organizational conduct, act of aiding and abetting have been broken.[295]

1.1 Dissimilation of Organizational Conduct

Under the case of CTOC, convenience and rapidity of information communication in the internet are also being used by criminals. Even though joint offenders do not contact face to face, with the internet they can co-ordinate their criminal acts in cyberspace. Obviously, the internet and ICTs can help the offenders of organizational conduct to reduce effort and time costs. In contrast, committing the same crime takes them more effort and time in the traditional real world.[296] As a matter of fact, in cyberspace when the offenders of organizational conduct organize crimes, they do not need to expose their real identity. And the other joint offenders are not under the arrangement and lead of these offenders of organizational conduct; the latter's role in this joint offence means that they only provide a chance to commit these crimes rather than they play the role of principal offenders in the real world. The most significant difference between the offenders of organizational conduct in cyberspace and in the real world is that they have obviously different functions. It can be said that organizational conduct is much easier to carry out in cyberspace. In these circumstances, some organizational conduct and abetment are converging with each other, namely, there is no clear boundary between them once they are carried out in cyberspace instead of in the real world. For example, the offenders of organizational conduct just instigate some unspecified persons to commit certain crime in cyberspace, but their act would successfully attract a great number of criminals to join that crime, and finally they commit that crime together. From the standpoint of traditional joint crime theory, it becomes a problem that these

[295] Yu Zhigang, *Research on the Dissimilation of Traditional Crime in the Internet Age*, China Procuratorial Press, 2010, p.37.
[296] In traditional criminal theory, organizing criminals are usually considered as the principle offenders.

types of act in cyberspace are categorised as organizational conduct or abetment. Except for this, another problem is that under traditional joint crime theory the offenders of organizational conduct are usually deemed as the principal offenders, but in cyberspace, the function and status of the offenders of organizational conduct in the whole crime are weakened. Gradually they have become accessories of CTOC. Of course, the dissimilation of organizational conduct does not exist in all types of CTOC. Taking a TOC as an example, which was detected by the Ministry of Public Security of the People's Republic of China on 24.Nov.2012, 9 foreign criminals in the territory of China accepted the instigation of foreign criminals outside China to commit online fraud from August of 2011, and the foreign victim corporations came from the USA, the United Arab Emirates and Spain, etc. One obvious character of this case is that all the joint offenders did not contact directly face to face in the real world, but actually they contacted the foreign offenders outside China via the internet.[297] Under the circumstances of this case, it is difficult to identify the behavior of foreign offenders outside China with organizational conduct or abetment, even though their behavior can be categorized as organizational conduct. It is also difficult to affirm that they play the role of principle criminals as this type of crime was committed in the real world.

1.2 Transformation of Aidant Act into Perpetrating Act

Compared with a perpetrating act, an aidant act is not necessary in a joint offence. In the case of cyber transnational organized crime, we can take the joint crime of forgery as an example. Before the internet age, in the real world as long as perpetrators complete the conduct of forging documents, the whole process of forgery was consummated in the crime. However, in the internet age, in order to prevent forging documents and to check certificates, the information of real certificates usually will be input to the related

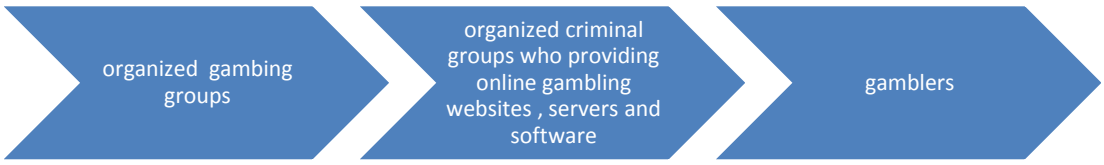
[297] On-line news, retrieved on 28.Apr.2014 from http://www.mps.gov.cn/n16/n1237/n2131945/3435067.html.

system of computers, and then the relative person can examine these certificates' authenticity on the internet. This change causes the whole process of forgery to have been prolonged correspondingly, which means if criminals want to forge some certain certificates and complete the whole process of forgery, they must break into the related computer system and input the corresponding forged information of certificates. From the viewpoint of traditional joint crime theory, the behavior of breaking into certain computer systems and inputting false information of relative certificates or documents was just aiding an act of forging certificates in the real world.[298] Actually in the internet era, in order to accept the relative persons examining the certificates' authenticity in the internet, most information on these certificates needs to be input into the relative computer systems after they are done in the real world,. According to this, the function of the behavior of inputting forging information concerning relative certificates promotes itself more significantly than the other conduct in the whole process of online forgery. And finally, the behavior of inputting forged information concerning relative certificates has become the most important and necessary step in the joint crime of forgery. On the contrary, under traditional joint crime theory, the behavior of inputting forged information concerning relative certificates is just an assisting act, but now in the internet age it has become perpetrating the act of forgery. The aiding act under the traditional joint crime theory is insufficient to access the nature and functions of breaking into a computer system and inputting the forged information of a certificate. In other words, if joint offenders commit transnational organized forgery in cyberspace, the conduct of breaking into a computer system and inputting false information of certificates has become the key step; actually this conduct has already been transformed into the act of perpetrating forgery instead of assisting behavior. In accordance with this change, the aiders of these crimes have become principal offenders.

[298] Yu Zhigang, *Research on the Dissimilation of Traditional Crime in the Internet Age*, China Procuratorial Press, 2010, p.39.

Another example is transnational online gambling, in 2010, the police of Shenzhen City cracked down an OCG across Hong Kong and mainland China. The members of this group provided online gambling groups with gambling websites, servers and software.[299] Compared with traditional gambling crimes, these conducts of providing online gambling websites, servers and software play a significant role in cyber gambling crimes, as they cannot be committed without this help. Obviously, an extra segment, providing online gambling websites, servers and software, differentiates organized online gambling from the organized gambling in the real world. There are three segments in organized online gambling, i.e., organized gambling groups, organized criminal groups who provide online gambling websites, servers and software and gamblers. This belongs to a chain structure, as figure 6 shows. This dissimilation means that the natures of aiding conducts have been changed. They evolve from aiding conduct to perpetrating acts, which also means aiders become perpetrators.

Figure 6: flow-process of organized online gambling



[299] On-line news, retrieved on 20. August.2014 from http://www.mps.gov.cn/n16/n1252/n1762/n2452/2461405.html

1.3 Vague Boundary between Aidant Act and Abetment

Some scholars hold the opinion that abetment should be not only limited as that it only can be committed via language. Certain conducts also can be considered as abetment, in fact they should be also criminalized as abetment.[300] In the following abetment will be categorized into language abetment and behavior abetment. In cyberspace behavior abetment more easily lures potential criminals to generate guilty intentions. For instance, under certain cyber transnational organized crimes, joint offenders provided some others with virus programs and Trojan-horse programs to carry out internet attacks, or tell some others that there are some defects with some network programs, and then they try to lure these persons to commit crimes via these defects in the internet. Under this condition, a problem was created, i.e., the act which is called the crime determination of potential criminals also significantly facilitates the implementation of this crime. According to the nature of these acts, there is no clear boundary between behavior abetment and the act of aiding. In other words, behavior abetment has both the nature of abetment and the aiding act. Under most countries' joint crime theories, abetment and aiding have been clearly differentiated with each other. The former mainly aims to create crime determination of potential criminals, without the instigation of abettors the potential criminals would not decide to commit crimes. In comparison with abetment, aidant acts target to ensure that the whole process of crime is completed smoothly. Just as in the circumstance that was discussed above, once the joint offenders tell some others that there are some defects with some certain network programs, and then lure these persons to commit crimes via these defects in the internet and provide them with virus programs and Trojan-horse programs, the boundary between abetment and aiding would become much vaguer than these crimes without the factor of the internet.

[300] Zhao Bingzhi and Zhang Xinping, attempted to Research on Cyber Joint Crime, issued by Tribune of Political Science and Law, No 5 of 2002.

2. Corresponding Solutions to Dissimilation of Joint Crime

Based on the above discussion of this section, obviously the de-hierarchy trend of cyber organized crimes are dissimilating the joint crime theory. Furthermore, one dilemma is manifested in judicial practice, as it is difficult to identify the role and function of each member in cyber organized criminal groups, so accordingly, it is not easy to define accurate criminal responsibilities of each offender. In order to solve these problems, the joint crime theory and judicial practices require some corresponding adjustments.

2.1 Criminalizing Organizational Conduct and Aidant Act as Perpetrating Act

It is deemed that organizational conduct plays a major role in joint offences under traditional criminal theory. But after the convergence of cybercrime and TOC, some organizational conduct and abetment are converging with each other. The corresponding problem is that there is no clear demarcation line between these two conducts. In cyberspace, the function and status of the offenders of organizational conduct in the whole crime are weakened, and gradually they have become accessories of cyber transnational organized crime. Another dissimilation problem is that by means of the internet, the aidant act has become the key part of the whole joint crime. Both dissimilation of organizational conduct and aidant act can be solved through criminalizing them as perpetrating acts. The major modus operandi is as follows:

Firstly, under a certain cyber transnational organized crime, one can examine whether the offenders of organizational conduct or aidant offenders contact the other joint offenders in the aspect of criminal intent. If there is a joint criminal intent between all of

joint offenders, it is no doubt that the offenders of organizational conduct or aidant offenders should be charged with criminal responsibility according to the same judiciary accusation as the other joint offenders.

Secondly, if there is no joint criminal intent between the offenders of organizational conduct or aidant offenders and the other joint offenders under certain CTOC. Criminalizing organizational conduct and aidant acts as perpetrating acts of another crime is a better way for getting out of this awkward situation. Because joint criminal intent is a necessary element in joint crime, on the contrary, without joint criminal intent, organizational conduct and aidant acts probably constitute the other crimes. In this condition, two situations need to be distinguished. One is that organizational conduct and aidant act do not harm new types of interests. It means that the interests which are harmed by these two types of act are already protected by existing criminal law. In the aspect of criminal intent, the offenders of organizational conduct or aidant offenders did not contact the offenders of such crimes, there are certain relationships between these criminals, but they are not joint offenders in the same crime. However, the offenders of organizational conduct or aidant offenders should be deemed to have committed another crime. So they should be individually indicted on charges of the existing accusation in criminal law according to their organizational conduct or aidant act. With respect to cyber transnational organized crime that is aided by organizational conduct or aidant act, in this situation, this aid is different from the aid in the joint crime, and it means that it indirectly helps this CTOC. The offenders of organizational conduct and aidant offenders should be charged with criminal liability according to another accusation that differentiates the accusation of this CTOC. In this sense, the organizational conduct or aidant act becomes the perpetrating act under the accusation by which they would be indicted. Another situation is that organizational conduct and aidant act harm a new type

of interests.[301] For instance, especially at early phase of the internet age, in some countries, stealing individual identity information was not crime. With the development of civil society, it is necessary to protect online individual identity information, and in this circumstance, online individual identity information is a new type of interest for these countries. Of course, at the moment, these new types of interests have not been protected by the domestic criminal law of the corresponding countries. These new interests, violated by organizational conduct or aidant act, need to be protected by criminal law, in a way which is always deemed the final defense for adjusting damaged social relationships in public.[302] In other words, the civil remedies are already not enough to adjust the damaged social relationships. Under this condition, on the one hand, the new interests need to be protected by criminal law. On the other hand, there are no available provisions laid down in criminal law that can be used to protect these new interests, but law enforcement agencies and judiciary systems need to comply with the doctrine of a legally prescribed crime. The offenders of organizational conduct or aidant offenders who infringe the new interest, in the aspect of criminal intent, do not have joint criminal intent with the other relative offenders of certain CTOC. So it is not fair if they are charged with the same criminal responsibilities with the relative offenders of certain CTOC. Otherwise, this modus operandi violates the doctrine of a legally prescribed crime. In other words, no criminal law means no criminal responsibility. So the scientific modus operandi is that of adopting new legislations to punish organizational conduct or aidant act. In this way organizational conduct or aidant act becomes a perpetrating act of a new judiciary accusation, namely, it is a way of solving dissimilation of organizational conduct or aidant act by criminalizing organization conduct and aidant act as perpetrating acts.

[301] It is difficult to give a concrete scope concerning the new type of interest, because maybe in one country one interest has not been protected by the existing criminal law, and it is necessary to give protection, so it can be said as a new legal interest. On the contrary, in another country this kind of interest is laid down in the criminal law..

[302] Criminal law usually is considered as the final defense means it is the last resort to remedy and adjust the damaged social relationships.

2.2 Criminalizing Aiders as Principals

Under the situation of cyber organized criminal groups (COCGs) with a chain structure, the function of aiders has been essentially changed by the internet and internet-related ICTs. According to traditional joint crime theory, the aiders should be considered as accessories in joint crimes. Once such crimes happen in cyberspace, such as organized online gambling, it could be committed without the aiders' "help". Actually, the function of aiders has been transferred into a principal role. One solution for this dissimilation is that the joint crime theory and judicial practice identify aiders as principals. Furthermore they should be imposed with criminal responsibility in accordance with the punishment principle for principals.

2.3 Criminalizing Abetment as Perpetrating Act

Under the traditional joint crime theory, abettors are usually imposed with criminal liability according to their role and function as joint offenders. For example the Chinese Criminal Code belongs to this type, the Article 29 of Chinese Criminal Code is the principle of punishment provision for the abettor.[303] However, the definition of aidant offenders cannot always be found in every country's criminal law. As a matter of fact, it usually exists in the joint crime theory. Sometimes, the definition of aidant offenders is replaced by the concept of accessory stipulated under corresponding provisions of criminal law. In cyberspace, the boundary between aidant act and abetment is not as clear as in the real world. Under a certain cyber transnational organized crime, some criminals provide others with virus programs and Trojan-horse programs to carry out internet attacks, or tell some others there are some defects with some certain network

[303] See the Article 29 of Chinese Criminal Code.

programs. By means of this they lure them to commit crimes via these defects. They abet potential criminals to commit TOC in cyberspace by means of behavior rather than language, which is different from the abettors under the traditional joint crime theory. This means that abetment takes on the characteristics of both the abetment and aidant acts.[304] Even though the boundary between abetment and aidant act in cyberspace is much vaguer than in the real world, the key point for solving this problem is that examining whether both of the two types of offenders had a joint criminal intent with the other joint offenders under one certain cyber transnational organized crime. Of course, if merits further research into how to investigate and determine that there is joint criminal intent between abettors and the other joint perpetrators in cyberspace; the standards about this also need to be established by theory of criminal law. In the following, the circumstances that abettors and the other joint offenders have joint criminal intent and no joint criminal intent will be analyzed.

If abettors had joint criminal intent with the other joint offenders in a certain case of CTOC, they should take criminal responsibility according to their role in the whole CTOC. Under this certain CTOC, the abettors may play both the role of abettor and aider based on their language abetment or behavior abetment, and both of their roles as abettor and aider need to be analyzed. Even though their acts are assessed twice, they could not be given double criminal liabilities due to one act. Namely, they only can be charged with one single criminal liability. In judicial practice aiders are always considered as accessories. Two circumstances need to be distinguished: One is that the abetment of abettors is assessed as taking a principle role in the whole CTOC, and then the abettors only should be imposed with criminal responsibility as principle perpetrators. Another circumstance is the abetment of abettors taking the role of accessory; it means that the abettors should be assessed as accessory under one certain

[304] Because the act of abettors also with the characteristic of aidant actors, for convenience, in the following of section 2.2, we call these criminals as abettors.

cyber transnational organized crime, and then they should be charged with the criminal liability of accessories.

If abettors did not have had joint criminal intent with the other joint offenders under one certain CTOC, in these circumstances, they are single crimes rather than joint crimes. So criminalizing the act of abettors as a perpetrating act is a better way for solving the dissimilation of abetment. And according to whether their abetment infringed upon a new type of interests, two circumstances need to be analyzed separately. The specific modus operandi are as follows: One is that abetment did not infringe on new interests, the interests which had been damaged by the abettors are protected by existing clauses of criminal law, then the abettors only should be charged with criminal responsibility in accordance with existing clauses which have been violated by the abettors, but it is an independent crime distinguished from the related CTOC. Another situation is that if the act of abettors infringed upon new type of interests, which are not protected by any existing provisions of criminal law, these new interests need to be protected by criminal law as the final remedy for the damaged social relationship. So the theory of criminal law should take account of the loopholes. Furthermore new legislation needs to be adopted to protect these new interests, such as by means of amendments, then adding new provisions under a given chapter of domestic criminal law.

Conclusion of Chapter 4

The main theme of this chapter analyzes the dilemmas of joint crime theory under cyber transnational organized crime, and proposes some resolutions to these dilemmas. It is obvious that structures of traditional organized crime are being changed by the internet. For example, as the analysis of section 1 of this chapter, in the internet age, the

structures of traditional organized crime have evolved from a Pyramid structure and Structure of Hub-and Spoke model into a Network structure, a Structure of aggregate ray and chain structure. The de-hierarchy trend among joint offenders as an accompanying phenomenon has emerged along with these changes. Accordingly, the de-hierarchy trend of traditional organized crime further transforms the functions and roles of every joint offender under some certain cyber transnational organized crimes. In contrast, under the situation of traditional joint crime theory, there are common agreements about the functions and roles of every joint offender in the criminal community. In order to solve the dissimilation about joint crime theory, section 2 proposes some solutions, such as criminalizing organizational conduct and the aidant act as a perpetrating act, criminalizing aiders as principals and criminalizing abetment as a perpetrating act. However, as proposals these solutions provide guides and directions with domestic criminal law and criminal theory. Furthermore the community dealing with criminal theory in a different country should adjust the joint crime theory in detail, according to the particular situation in their countries.

Chapter 5 Conflicts of Jurisdiction and Corresponding solutions of Transnational Organized Crime in the Internet Era

Conflicts of jurisdiction are the other problems brought to criminal theory and judicial practices by the Internet and internet-related ICTs. Normally TOC involves at least two countries, once all involved countries claim criminal jurisdiction over such case, conflicts of jurisdiction would be inevitable. Furthermore, combination of transnational organized crime and internet and internet-related ICTs make these conflicts more complicated. This chapter will analyze these conflicts and give some proposals to solve the problems.

Section 1 Conflicts of Jurisdiction of Transnational Organized Crime in the Cyber Age

In real world, since the border of physical space is clear, in accordance with such feature of physical space the jurisdiction of TOC is also explicit, countries that involving one transnational organized crime can claim criminal jurisdiction according to some given jurisdiction doctrines[305] within certain territory. In contrast, the border of cyberspace is ambiguous, almost all factors in cyberspace related to one certain CTOC are manifested as information data, there are rare tangible physical objects which can be used to determine jurisdiction. Actually, it is difficult to divide cyberspace into certain parts and distribute them to different countries, which further results in disorder and confusion when determine jurisdiction of CTOC. In view of this situation this section will analyze the conflicts of jurisdiction under CTOC.

[305] They include territorial criminal jurisdiction, personal criminal jurisdiction, protective criminal jurisdiction and universal criminal jurisdiction, the factors related to these doctrines are explicit things and objects, such as property, behavior, nationality.

1. Criminal Jurisdiction Doctrine

Traditional criminal jurisdiction doctrines include territorial criminal jurisdiction, personal criminal jurisdiction, protective criminal jurisdiction and universal criminal jurisdiction:[306] (1) Territorial criminal jurisdiction refers to a nation has absolute and exclusive criminal jurisdiction over every person, events and things related to crimes within its territory; (2) Personal criminal jurisdiction means that a nation has criminal jurisdiction over the nature persons and legal persons who have its nationality once they commit crimes outside its territory;[307] (3) once a crime threatens a nation's security, basic functions or the interests of its citizens, protective criminal jurisdiction allows it to exercise criminal jurisdiction when this crime occurs outside of its territory;[308] (4) Universal criminal jurisdiction only can be applied to certain limited crimes which stipulated in certain regional and international conventions, related countries can only claim universal criminal jurisdiction once such crimes happened, regardless of the location of act, nationality of the perpetrator or victim, or the related protected interests belonging to which country.[309] Generally speaking, majority of countries take such criterion about criminal jurisdiction, namely, taking territorial criminal jurisdiction as the principal criterion, by contrast, personal criminal jurisdiction, protective criminal jurisdiction and universal criminal jurisdiction as the supplement criteria. Before the interaction and integration of TOC and cyber crime, these principles can successfully solve criminal jurisdiction problems when combating transnational organized crimes,

---

306 Qu Xinjiu eds. *Science of Criminal Law*, China University of Political Science and Law Press, issued 2008. P.18.

307 Ibid.

308 Ibid.

309 supra § II. See also Restatement (Third) of Foreign Relations Law of the United States § 404 (1987) ("A state has jurisdiction to define and prescribe punishment for certain offenses recognized by the community of nations as of universal concern, such as piracy, slave trade, attacks on or hijacking of aircraft, genocide, war crimes, and perhaps certain acts of terrorism, even where none of the bases of jurisdiction indicated in § 402 is present"). Cf. United States v. Yousef, 327 F.3d 56, 99-100 (2d Cir. 2003) (district court improperly found it could exercise universal jurisdiction over terrorist activities). See in Susan W. Brenner and Bert-Jaap Koops, Approaches to Jurisdiction Cybercrime, 2004 Journal of High Technology Law, Vol. IV No. 1.2004.

protecting human rights, defending state interests and avoiding international jurisdiction conflicts. However, with the proliferation of the internet and internet-related ICTs, OCGs are also exploiting ICTs, combining with instantaneous and limitless characters of cyberspace, which brought strong challenges to these four criminal jurisdiction principles. Under the circumstance of traditional transnational organized crime, it is easy to determine criminal jurisdiction according to the location of criminal behavior or criminal results. Under the traditional criminal jurisdiction principles, the traditional conjunctive factors that are used to determine the criminal jurisdiction include location of criminal behavior or result, and nationalities, and so on. By contrast, under the situation of cyber transnational organized crimes, criminal behavior and criminal results usually are located in different countries, even to be exact they are committed in cyberspace which is significantly different from in physical space. In order to protect their national and citizens' interests, every involved country wants to expand its jurisdiction over cyber transnational organized crimes. Obviously, under such conditions traditional conjunctive factors are insufficient to be used to determine criminal jurisdiction over CTOC. Except for location of criminal behavior and criminal results, some new conjunctive factors, such as website address, the place where internet data are browsed or downloaded and the internet node where computer data arrive at or pass are already be used to determine criminal jurisdiction. Beyond all doubt, these judicial practices have resulted in positive and negative conflicts of criminal jurisdiction over CTOC.

2. New Conjunctive Factors to Determine Criminal Jurisdiction of Cyber Transnational Organized Crimes

Under the four traditional criminal jurisdiction doctrines, the conjunctive factors to determine criminal jurisdiction include the location of criminal conduct and

consequences, the nationalities of offenders or victims, the interests of one country or its citizens when they are victims, and if some particular crimes regulated in certain international conventions, their member states can claim criminal jurisdiction by means of their conventional responsibilities. By contrast, the offenders of cyber transnational organized crimes carry out their conduct in cyberspace via the internet or internet-related ICTs, the factors under these crimes are significantly difference with the traditional conjunctive factors. In order to be compatible with these changes, some countries began to use some new conjunctive factors to establish connections to criminal jurisdiction of cybercrimes or cyber transnational organized crimes. These new conjunctive factors include location of website address, location of servers, and locations where internet signal or data transmit, pass or arrive at. The establishment of these new conjunctive factors has been indicated by legislations of certain countries to expand criminal jurisdiction over cybercrime or CTOC.

3. **Legislation to Expand Criminal Jurisdiction**

Positive conflicts of jurisdiction concerning cybercrime can be reflected at the respect of different countries expanding to exercise their jurisdiction over such type of crimes. Some countries' jurisdiction clauses under their criminal law against cybercrime will be analyzed at the aspect of their expansive jurisdiction over cybercrime:

Jurisdiction clauses about cybercrime in the United States. Firstly, at the respect of territorial jurisdiction, several states take a very abroad approach to the issue of cybercrime jurisdiction. The jurisdiction provision of Arkansas' computer crime legislation states that "a person is subject to prosecution in this state for any conduct proscribed by this subchapter, if the transmission that constitutes the offense either

originates in this state or is received in this state."[310] Connecticut's cybercrimes code states its jurisdiction provision that if "any act performed in furtherance of the offense" defined by the code "occurs in this state or if any computer system or part thereof accessed in violation of" the computer crimes code "is located in this state, the offense shall be deemed to have occurred in this state."[311] North Carolina's equivalent provision states that any offense defined by its computer crimes code is "committed by the use of electronic communication may be deemed to have been committed where the electronic communication was originally sent or where it was originally received in this State."[312] Utah relies on statutes defining general criminal jurisdiction to establish jurisdiction in cybercrime cases.[313] The statute of Utah provides as follows: (1) A person is subject to prosecution in this state for an offense which he commits, while either within or outside the state, by his own conduct or that of another for which he is legally accountable, if: (a) the offense is committed either wholly or partly within the state; (b) the conduct outside the state constitutes an attempt to commit an offense within the state; (c) the conduct outside the state constitutes a conspiracy to commit an offense within the state and an act in furtherance of the conspiracy occurs in the state; or (d) the conduct within the state constitutes an attempt, solicitation, or conspiracy to commit in another jurisdiction an offense under the laws of both this state and such other jurisdiction. (2) An offense is committed partly within this state if either the conduct which is any element of the offense, or the result which is such an element, occurs within this state.[314] The most expansive U.S. state provision is found in the provisions of the West Virginia Computer Crimes and Abuse Act, which added the following section to the West Virginia criminal code: Any person who violates any provision of this "computer

[310] Ark. Code Ann. § 5-27-606 (2003). See in Susan W. Brenner and Bert-Jaap Koops ,Approaches to Jurisdiction Cybercrime, 2004 Journal of High Technology Law, Vol. IV No. 1.2004.
[311] Conn. Gen. Stat. Ann. § 53a-261 (2004). See Susan W. Brenner and Bert-Jaap Koops ,Approaches to Jurisdiction Cybercrime, 2004 Journal of High Technology Law, Vol. IV No. 1.2004.
[312] N.C. Gen. Stat. § 14-453.2 (2002). See Susan W. Brenner and Bert-Jaap Koops ,Approaches to Jurisdiction Cybercrime, 2004 Journal of High Technology Law, Vol. IV No. 1.2004.
[313] See Oh. Rev. Code Ann. § 2901.11 & Utah Code Ann. § 76-1-201(2003). See Susan W. Brenner and Bert-Jaap Koops ,Approaches to Jurisdiction Cybercrime, 2004 Journal of High Technology Law, Vol. IV No. 1.2004.
[314] Utah Code Ann. § 76-1-201 (2003). See Susan W. Brenner and Bert-Jaap Koops ,Approaches to Jurisdiction Cybercrime, 2004 Journal of High Technology Law, Vol. IV No. 1.2004.

crimes code" and, in doing so, accesses, permits access to, causes access to or attempts to access a computer, computer network, computer data, computer resources, computer software or computer program which is located, in whole or in part, within this state, or passes through this state in transit, shall be subject to criminal prosecution and punishment in this state and to the civil jurisdiction of the courts of this state.[315] Michigan's general criminal jurisdiction statute, declares that the state can prosecute someone who, "while physically located within this state or outside of this state," commits a criminal offense that "produces substantial and detrimental effects within this state."[316] At the federal level, as § V(A), infra, explains in detail, the United States' basic federal computer crimes provision –18 U.S. Code § 1030 – allows the U.S. government to exercise jurisdiction over criminal activity that "affects interstate or foreign commerce or communication of the United States."[317] Secondly, in the aspect of personality jurisdiction, the basic federal cybercrime provision – 18 U.S. Code § 1030 – confers jurisdiction to prosecute when the conduct at issue impacts upon the federal government, i.e., where the United States is itself the victim. Section 1030(a) (3) of title 18 of the U.S. Code, for example, makes it a federal offense for anyone "intentionally, without authorization to access any nonpublic computer of a department or agency of the United States." And section 1030(a) (6) (B) makes it a federal crime to "knowingly and with intent to defraud," or traffic in any password that can be used to access a computer that is used "by or for the Government of the United States."[318] Thirdly, in the aspect of protective jurisdiction, The United States' basic federal computer crimes provision, 18 U.S. Code § 1030 was added by the USA Patriot Act, enacted in October, 2001, specifically to confer extraterritorial jurisdiction in cybercrime cases.

[315] W. Va. Code Ann. § 61-3C-20 (2004). See Susan W. Brenner and Bert-Jaap Koops ,Approaches to Jurisdiction Cybercrime, 2004 Journal of High Technology Law, Vol. IV No. 1.2004.
[316] State v. Dudley, 354 S.C. 514, 581 S.E.2d 171 (2003); People v. Blume, 443 Mich. 476, 505 N.W.2d 843 (Mich. 1993). See Susan W. Brenner and Bert-Jaap Koops ,Approaches to Jurisdiction Cybercrime, 2004 Journal of High Technology Law, Vol. IV No. 1.2004.
[317] 18 U.S. Code § 1030(e)(2)(B) (2004). See Susan W. Brenner and Bert-Jaap Koops ,Approaches to Jurisdiction Cybercrime, 2004 Journal of High Technology Law, Vol. IV No. 1.2004.
[318] Susan W. Brenner and Bert-Jaap Koops ,Approaches to Jurisdiction Cybercrime, 2004 Journal of High Technology Law, Vol. IV No. 1.2004.

It states that the Act amends the definition of 'protected computer' to make clear that this term includes computers outside of the United States so long as they affect 'interstate or foreign commerce or communication of the United States.' The United States can now use speedier domestic procedures to join in international hacker investigations. As these crimes often involve investigators and victims in more than one country, fostering international law enforcement cooperation is essential.[319] Finally, the federal government of the United States relies on the notion of universal jurisdiction with regard to only a few crimes, including piracy, hostage-taking, aircraft hijacking, aircraft sabotage and torture.[320]

Jurisdiction clause of cybercrime in Netherlands. Art. 2 of Dutch Criminal Code concerns the territorial jurisdiction. It states that the Code "is applicable to anyone guilty of any offense in the Netherlands".[321] Netherlands also has number of personality jurisdiction provisions concerning specific cybercrime. For instance, forgery, including computer forgery, committed abroad by Dutch government employees or employees of international organizations located in the Netherlands is punishable in the Netherlands, if the act is punishable in the country where it was committed;[322] computer sabotage or data damage committed against a Dutch national if the act is covered by article 2 of the International Convention for the Suppression of Terrorist Bombings;[323] or if it is covered by article 2 of the International Convention for the Suppression of the Financing of Terrorism.[324]

---

[319] Ibid.

[320] Wayne R. LaFave, SUBSTANTIVE CRIMINAL LAW § 4.3(e) (2003). See Susan W. Brenner and Bert-Jaap Koops ,Approaches to Jurisdiction Cybercrime, 2004 Journal of High Technology Law, Vol. IV No. 1.2004.

[321] Susan W. Brenner and Bert-Jaap Koops ,Approaches to Jurisdiction Cybercrime, 2004 Journal of High Technology Law, Vol. IV No. 1.2004.

[322] Art. 4(11) jo. 225 Wetboek van Strafrecht (Dutch CC). See Susan W. Brenner and Bert-Jaap Koops ,Approaches to Jurisdiction Cybercrime, 2004 Journal of High Technology Law, Vol. IV No. 1.2004.

[323] Art. 4(13) Wetboek van Strafrecht (Dutch CC). International Convention for the Suppression of Terrorist Bombings, New York, 15 December 1997. See Susan W. Brenner and Bert-Jaap Koops ,Approaches to Jurisdiction Cybercrime, 2004 Journal of High Technology Law, Vol. IV No. 1.2004.

[324] Art. 4(14) jo. 161sexies and 350a Wetboek van Strafrecht (Dutch CC). International Convention for the Suppression of the Financing of Terrorism, New York, 9 December 1999. See Susan W. Brenner and Bert-Jaap Koops ,Approaches to Jurisdiction Cybercrime, 2004 Journal of High Technology Law, Vol. IV No. 1.2004.

·Jurisdiction clause of cybercrime in Germany. In the aspect of territorial jurisdiction provision, the German Criminal Code further details when an act is considered to have been committed on the territory of Germany: (1) An act is committed at every place the perpetrator acted or, in case of an omission, should have acted, or at which the result, which is an element of the offense, occurs or should occur according to the understanding of the perpetrator; (2) Incitement or accessoryship is committed not only at the place where the act was committed, but also at every place where the inciter or accessory acted or, in case of an omission, should have acted or where, according to his understanding, the act should have been committed. If the inciter or accessory in an act abroad acted domestically, then German criminal law shall apply to the incitement or accessoryship, even if the act is not punishable according to the law of the place of its commission.[325] At the respect of personality jurisdiction clause, Germany has a comparable general provision which based on the nationality of the perpetrators: it has jurisdiction over a crime committed abroad by a German national if the act is punishable where it was committed or is not subject to criminal jurisdiction where it was committed.[326] Another jurisdiction provision based on the nationality of the victims provides that a crime committed against a German national if the crime is punishable in the country where it was committed or is not subject to a criminal jurisdiction where it was committed.[327] In the aspect of universality jurisdiction, Germany does claim universal jurisdiction for a particular cybercrime: child pornography.

·Jurisdiction clause of cybercrime in Malaysia. Malaysia's Computer Crime Act is even less limited than Singapore's: (1) The provisions of this Act shall, in relation to any person, whatever his nationality or citizenship, have effect outside as well as within Malaysia, and where an offence under this Act is committed by any person in

[325] § 9(2) Strafgesetzbuch (German CC). See Susan W. Brenner and Bert-Jaap Koops ,Approaches to Jurisdiction Cybercrime, 2004 Journal of High Technology Law, Vol. IV No. 1.2004.
[326] § 7 Nr. (2)(1) StGB.Strafgesetzbuch (German CC). See Susan W. Brenner and Bert-Jaap Koops ,Approaches to Jurisdiction Cybercrime, 2004 Journal of High Technology Law, Vol. IV No. 1.2004.
[327] §7 Nr. (2)(1) StGB. See Susan W. Brenner and Bert-Jaap Koops ,Approaches to Jurisdiction Cybercrime, 2004 Journal of High Technology Law, Vol. IV No. 1.2004.

any place outside Malaysia, he may be dealt with in respect of such offence as if it was committed at any place within Malaysia. (2) For the purposes of subsection (1), this Act shall apply if, for the offence in question, the computer, program or data was in Malaysia or capable of being connected to or sent to or used by or with a computer in Malaysia at the material time.[328]

Jurisdiction clause of cybercrime in Singapore. Singapore has wide-reaching jurisdiction clause in their computer crime statutes. The provision reads as following: Territorial scope of offences under this Act: 11. (1) Subject to subsection (2), the provisions of this Act shall have effect, in relation to any person, whatever his nationality or citizenship, outside as well as within Singapore. (2) Where an offence under this Act is committed by any person in any place outside Singapore, he may be dealt with as if the offence had been committed within Singapore. (3) For the purposes of this section, this Act shall apply if, for the offence in question (a) the accused was in Singapore at the material time; or (b) the computer, program or data was in Singapore at the material time.[329]

Obviously, the aforementioned clauses concerning criminal jurisdiction of cybercrime have been over expanded at different extent, accordingly these clauses created new connection points which are used to determine criminal jurisdiction. By contrast, ordinary criminal law usually does not touch new standard of determining criminal jurisdiction concerning cybercrime.

According to the jurisdiction clauses over cybercrime and different theories concerning criminal jurisdiction over cybercrime, a great number of countries have expanded their

[328] Art. 9 Malaysia Computer Crimes Act. See Susan W. Brenner and Bert-Jaap Koops ,Approaches to Jurisdiction Cybercrime, 2004 Journal of High Technology Law, Vol. IV No. 1.2004.
[329] Art. 11 Singapore Computer Misuse Act. See Susan W. Brenner and Bert-Jaap Koops ,Approaches to Jurisdiction Cybercrime, 2004 Journal of High Technology Law, ISSN 1536-7983.

criminal jurisdiction over cybercrimes. The aforementioned jurisdiction clauses provide examples which mainly reflect positive conflict of cybercrime jurisdiction. Obviously, positive conflict of criminal jurisdiction over cybercrime mainly results from different countries excessively expanding and claiming to exercise their criminal jurisdiction over such cases. In order to solve the positive conflicts of criminal jurisdiction over cybercrime which are caused by different countries excessively expanding and claiming to exercise their criminal jurisdiction concerning cybercrime, scholars and researchers proposed a great number of theories: Some scholars hold theory of new sovereignty, which propose cyberspace should separate itself from the governments of real world and possess autonomy, and based on this one set of independent judicial system should be established;[330] some scholars even propose cyberspace should be considered as international space like Antarctica, outer space and international waters.[331] Some researchers hold that universality jurisdiction should be exercised over cybercrime.[332] The other jurisdiction theories include the original country of website and location of servers, both of them can be applied for claiming criminal jurisdiction over related CTOC. In German criminal community theories of limiting location of criminal result and double criminality have been proposed to solve the jurisdiction about cyber crime, because in the past judicial practice German courts excessively expanded their jurisdiction of cybercrime according to the § 9 (2) Strafgesetzbuch (German CC). In order to restrict the trend of over expanding jurisdiction over cybercrime, the theory of limiting location of criminal result proposes that only under the condition that foreign criminals intend to commit criminal result in one country, or the criminals already fully realize the criminal result will be definitely generated in corresponding countries, but they continue to commit this cybercrime, territorial jurisdiction can be applied over this cybercrime.[333] Among Chinese criminal theory, some scholars propose the connected

[330] See Yu Zhigang, The Age of Informationalized Transnational Crime and Chinese Choice concerning The Council of Europe Convention on Cybercrime. Legal Forum, Issue 2, 2013.
[331] Ibid.
[332] Han Zhe, the Substantive Characteristics and Criminal Jurisdiction of Cybercrime, Journal of Shandong Police College, Issue 3. 2003, p.71.
[333] See Yu Zhigang, The Age of Informationalized Transnational Crime and Chinese Choice concerning The Council of Europe Convention on Cybercrime. Legal Forum, Issue 2, 2013.

principle in accordance to substantive damage over cyber crime jurisdiction, which means among all the involved countries only the countries that suffer substantive damage have the right to claim jurisdiction over certain cyber crime. Actually this principle can be applied to CTOC as well, and it is a relatively better resolution to solve positive conflict of cybercrime and CTOC over jurisdiction. In section 2 we will analyze it in detail.

4. Positive Conflicts of Jurisdiction

Since computer data are transmitted instantaneously between different countries, location of criminal act and location of criminal consequences may be located in a great number of countries. Under this condition more than two countries may assert criminal jurisdiction to a related CTOC. But compared with traditional transnational organized crime, under CTOC, in addition to location of criminal behavior and criminal results, the other conjunctive factors, like the website address, the place where internet data are browsed or downloaded and the internet node where computer data arrive at or pass are already be used to determine criminal jurisdiction. And if all the involved countries would claim criminal jurisdiction over this crime, positive conflicts of jurisdiction would be created therewith. As a matter of fact, it is not reasonable that all the new conjunctive factors can be used to determine criminal jurisdiction. Both of practitioners and scholars expressed their suspicion and worries about blind expansion of criminal jurisdiction of cyber crime and CTOC worldwide. The limitless criminal jurisdiction will lead to a circumstance that every country can assert criminal jurisdiction over related cyber transnational organized crime.[334] Does this not only excessively invade

[334] Yu Zhigang, The Age of Informationalized Transnational Crime and Chinese Choice concerning The Council of Europe Convention on Cybercrime, Legal Forum, Issue 2, 2013.

legal rights and interests of offenders, but also sharply impacts traditional national judicial supremacy.

5. Negative Conflicts of Jurisdiction

The damage of CTOC can be beyond territory of one country due to the limitless character of internet, even though there are many differences between different countries' criminal legislations. Accordingly, these different domestic legislations can lead to the negative conflicts over CTOC. For example, under some countries' domestic criminal law, the conducts of TOCGs are criminalized as crime, while so do some other countries not. Finally, if all the involved countries do not punished such serious crimes, there is no sovereign state prosecuting these types of TOC. For example, on 4.MAY.2000 a computer virus named "I love you" was widespread worldwide via email of Microsoft Outlook, many departments of American National Defense, the Parliament of the United Kingdom and a great number of transnational corporations were infected with this virus.[335] Even thought there were evidences proving that this computer virus came from Philippines, and police of Philippines also arrested the creator of this virus, there was no corresponding law can be applied to punish the conduct of this creator. Finally, the department of Philippine judicial practice quashed this indictment.[336] Such kind of case rightly reflects negative conflicts of jurisdiction about cyber crime, and probably this situation would happen under cyber transnational organized crimes. Because the gaps between differences of domestic criminal laws are being used by criminals of CTOC and cyber crime as a shield of circumventing penal sanction, which would cause a large increase about the number of negative conflicts jurisdiction.

[335] On-line news, Retrieved on 28. Apr. 2014 from http://tech.sina.com.cn/roll/2008-12-07/1706902529.shtml.

[336] Gong Yanmei, Network Crime Jurisdiction Conflicts and Determine, Master dissertation, published by Lanzhou University, 2012.

Section 2 Corresponding Solutions of Conflicts of Jurisdiction of Transnational Organized Crime in the Internet Era

Section 1 discussed the jurisdiction under related legislations of some countries over cybercrimes and cyber transnational organized crimes, which are the reflections of the over-expanding jurisdiction over cyber crime and CTOC. In view of this satiation, it can be said that positive conflicts of criminal jurisdiction result from the over-expanding jurisdiction and negative conflicts are brought by legislative absences. Accordingly, this section will introduce some perspectives in criminal community about how to solve jurisdiction conflicts of cyber crime and CTOC, and analyze a relative reasonable resolution held by this dissertation.

1. Theories of solving Jurisdiction Conflicts of Cyber Transnational Organized Crime

Internet should not be used by OCGs as the instrument to avoid criminal sanctions, cyberspace also should not be vacuum of national criminal jurisdiction.[337] However, a basic principle must be observed, which is that any sovereign country cannot apply its criminal laws to the crimes occurring within the physical territory of another country. Just as the U.S. Supreme Court said in American Banana Company v. United Fruit Company, 213 U.S. 347, 356 (1909), "the character of an act as lawful or unlawful must be determined wholly by the law of the country where the act is done."[338] However,

[337] It is manifested at the aspect of negative conflicts of criminal jurisdiction of cyber transnational organized crimes

[338] See, e.g., The Apollon, 22 U.S.(9 Wheat) 362,371(1824). See also United Nations Convention against Transnational Organized Crime, Article 4("Protection of Sovereignty") (2000), availalbe at http://www.uncjin.org/Doucuments/Conventions/dcatoc/final_documents_2/convention_eng.pdf. See generally RESTATEMENT(THIRD) OF FOREIGN RELATIONS LAW OF THE UNITED STATES §206 cmt. b (1987).

rapidness and borderless characters of internet aggravate jurisdiction conflicts concerning cyber crime and CTOC. Just as Susan W. Brenner and Bert-Jaap Koops said that cybercrime statutes which have been enacted over the past decades in innumerous countries show varying and diverging jurisdiction clauses.[339] Since varying and diverging jurisdiction clause laid down in criminal law against cybercrime, coupled with there is no unified standard solving these conflicts of jurisdiction concerning cybercrimes or even CTOC, positive and negative jurisdiction conflicts of cybercrime and CTOC have brought to us. What's worse is that these problems having significantly affected the effect of combating CTOC.[340] Next some resolutions will be proposed to solve the conflicts concerning cyber transnational organized crimes.

1.1 Relative Theories of Establishing Jurisdiction about Cybercrime

CTOC is one sub-concept of cybercrime, so the relative theories of establishing jurisdiction about cybercrime also can be applied to CTOC. In the traditional criminal theory, the location of criminal behavior and criminal result are usually considered as the main conjunctive factors for determining criminal jurisdiction. By contrast, in the internet age, the conjunctive factors which are used to claim criminal jurisdiction have not been limited as before. New conjunctive factors include website address and internet nodes where the online data arrive at or pass, etc, which are used to determine the criminal jurisdiction under certain theories for establishing jurisdiction over cybercrime.

1.1.1 Theory of New Sovereignty

[339] Susan W. Brenner and Bert-Jaap Koops ,Approaches to Jurisdiction Cybercrime, 2004 Journal of High Technology Law, Vol. IV No. 1.2004.

[340] Even though majority of countries did not laid down jurisdiction clause about cyber transnational organized crime, the jurisdiction clause concerning cybercrime usually can be applied to cyber transnational organized crime, because this dissertation holds that cyber transnational organized crime is a sub-category of cybercrime.

Since cyberspace has the characters of transnational, on-limits and centerless, the theory of new sovereignty, also named as the theory of internet self-government or the theory of self-jurisdiction, considers that cyber space is an entirety, special zone without clear boundary, so a new sovereignty should be established in cyberspace. American scholar Mark Poster and some other scholars support this theory.[341] They hold that cyber space is an independent society system with its own rules, which should be distinguished from real world. Accordingly, this society has its own absolutely autonomous rights, the ways that how to organize itself and its own value standard. Specifically, the jurisdiction in cyber space should be solved by the following ways: the disputes and crimes between internet users only follow regulations which are formulated by the IPS (internet service provider), in cyberspace, only internet service providers arbitrate these conflicts as amiable compositer and can implement the arbitration.[342]

The theory of new sovereignty was created at the early phase of researching on criminal jurisdiction over cybercrime. However, the internet and internet-related ICTs are operated by natural persons, this theory separates the close relationship between cyberspace and real world, neglects national sovereignty and the objectivity of internet. According to this theory, it is impossible and unpractical to completely solve all kinds of conflicts of interest in cyber space. Finally, the operation system, designed by this theory, possibly will result in confusion and disorder when solving conflicts of jurisdiction about cybercrimes.

1.1.2 Theory of Website Address Jurisdiction

Some scholars proposed the theory of website address jurisdiction, they argued that website address is a relatively constant and stable factor in internet, so website address can be utilized to determine criminal jurisdiction of cybercrime.[343] However, this

[341] Wang Shuai, Jurisdiction about Cyber-crime, Master dissertation, published by Liaoning University, 2012.
[342] Gong Yanmei, Network Crime Jurisdiction Conflicts and Determine, Master dissertation, published by Lanzhou University, 2012.
[343] Chen Qi, Research on the Jurisdiction Problem of Online Tort Disputes, Journal of Jimei University, Philosophy and Social Sciences Edition, 2006, Issue 1.

theory still has weaknesses: It does not realize such a fact that criminals usually input false information in internet. Meanwhile they can hide their website address with the help of ICTs, usually, it is not coincident that the location of website address and the location of possessor of this corresponding website address. This fact makes the criminals often cannot be easily detected by police, which means the theory of website address jurisdiction will be meaningless.

1.1.3 Theory of Expanding Territorial Jurisdiction

Territorial jurisdiction is a traditional principle of jurisdiction. But in the internet age, it is not enough to cover the criminal jurisdiction of majority of cybercrimes. In order to improve this situation and protect its national and civil interests at the maximum extent, almost every country tries to expand its own criminal jurisdiction over cybercrime. According to this trend, the theory of expanding territorial jurisdiction was proposed to cope with criminal jurisdiction of cybercrime. This theory takes traditional principle of territorial jurisdiction as basis, and it proposes that the standard of location of criminal behavior and criminal result should be expand. For example, it advocates that taking the location of downloading online data as conjunctive factor to determine criminal jurisdiction of cybercrime.[344] For instance, the Graham · Vodin case in the United Kingdom in 1999, Vodin is a business man, 28 years old and lives in Sutton of the United Kingdom, he established a pornographic website with the server that located in the USA and operated it in his Sutton house. He charged 25 pound per visitor. The police of the United Kingdom found his pornographic website and prosecuted Vodin to court. Vodin argued that his website was established in the USA, the contents of this pornography were published in the USA instead of the United Kingdom. But the judge did not adopt his arguments. On the contrary, the judge thought this pornographic data were downloaded by the British police in the territory of the United Kingdom, base on this the court had criminal jurisdiction over this case.[345]

[344] Gong Yanmei, Network Crime Jurisdiction Conflicts and Determine, Master dissertation, published by Lanzhou University, 2012.

[345] Qu Xuewu, on-line article, retrieved on 29.Apr.2014 from http://www.chinalawedu.com/news/16900/173/2004/9/re55364858341419400221750_132125.htm.

Of course, the theory of expanding territorial jurisdiction can protect corresponding countries' national and civil interests at the maximum extent. However, sometimes it would over-expand territorial jurisdiction over cybercrime and CTOC. For example, some unreasonable conjunctive factors even are used to determine criminal jurisdiction of cybercrime, like internet node where internet data just pass by, but this do not cause any damage to corresponding countries, it is not reasonable that the corresponding countries claim criminal jurisdiction based on the fact that the internet single pass by their territory, actually, this situation means that the corresponding countries over-expand their criminal jurisdiction over the related crime.

1.1.4 Theory of Limited Criminal Jurisdiction

The theory of limited criminal jurisdiction was proposed by some Chinese scholars. They advocate that criminal jurisdiction of cybercrime should be established on the base of personal jurisdiction, on the basis of damage result from cybercrime and relevance between cybercrime and corresponding countries, under this condition criminal jurisdiction can be established.[346] However, on the one hand, this theory neglects that territorial jurisdiction is the most important principle of jurisdiction rather than personal jurisdiction. On the other hand, the relevance standard in this theory is not clear, and it is difficult to implement it in judicial practice.

1.1.5 Theory of Limiting the Location of Criminal Result

The theory of limiting the location of criminal result was proposed by some German scholars. The aim of this theory mainly restricts over expansion of territorial jurisdiction over cybercrime. And this theory proposes that the location of criminal result of cybercrime should be strictly explained in judicial practice. In another word, only

[346] Gong Yanmei, Network Crime Jurisdiction Conflicts and Determine, Master dissertation, published by Lanzhou University, 2012.

foreign criminals intently commit criminal result in one country's territory, or these offenders have fully realized that this criminal result will possibly generate in corresponding country, only these conditions are satisfied, territorial jurisdiction can be applied over this cybercrime.[347] This theory takes territorial jurisdiction as its basis, and it can relatively reasonable solve the conflicts of criminal jurisdiction over cybercrime.

2. Effective Resolution to Positive Conflicts of Jurisdiction

This part discusses the theory, connected principle in accordance to substantive damage, held by this dissertation to solve positive conflicts of jurisdiction. This principle was proposed by Yu Zhigang in his article, the Age of Informationalized Transnational Crime and Chinese Choice concerning The Council of Europe Convention on Cybercrime. In view of the present situation of overexpansion of jurisdiction about cybercrimes, this theory was proposed to establish a reasonable and modest principle about jurisdiction of cybercrime. The following text will analyze its content, foundation and how to apply it in judicial practical.

2.1 Foundation of Connected Principle in Accordance to Substantive Damage

The foundation of connected principle in accordance to substantive damage should be explained on the base of territorial jurisdiction instead of the other jurisdiction principles. For example, if OCGs commit CTOC in one country targeting another country, the first country is the location of the act, and the second is the location of result.[348] In other words, the OCGs fully utilized the borderless feature of internet when

[347] See Hiroyuki Matsumoto eds. *Internet, Information Society and Law-the German and Japanese Symposium*, cited in Zheng Shanzhe, Cybercrime and the Principle of Territorial Criminal Jurisdiction, Chinese Journal of Law, 2006, issued 5.

[348] The act was not criminalized by the location of act, but this act was criminalized by the location of result.

they committed the crime, once the location of the act do not punish such act, only the location of result penalize their act, but the offenders are at the location of the act, under this situation they can escape the criminal responsibility, actually they on purpose take advantage of national boundary of criminal law's spatial validity. When the country which is the location of criminal result claims jurisdiction over this crime, it should rely on territorial jurisdiction principle instead of protective jurisdiction principle, because protective jurisdiction principle requires double criminality.[349] If the country which the location of criminal result claims jurisdiction based on protective jurisdiction principle, under the condition that once this act was not criminalized by criminal law of the location of act, it would have no right to exercise jurisdiction over this case due to the existence of double criminality. However, such awkward situation would not exist, if the country which is the location of result applied criminal jurisdiction according to territorial jurisdiction which do not require double criminality. So it is much reasonable that the territorial jurisdiction was explained as the foundation of connected principle in accordance to substantive damage.

2.2 Content of Connected Principle in Accordance to Substantive Damage

As for the content of connected principle in accordance to substantive damage, two elements should be taken into account, namely, both of the objective and subjective elements should be included in the scope of content. On the one hand, in the objective aspect, the act under a CTOC must result in substantive damage to the country which wants to exercise its criminal jurisdiction over this CTOC. Thereafter a question is given rise to, what are the content of the substantive damage? The substantive interests

[349] Once a country claimed protective jurisdiction, it is very that under the situation the criminals are non-citizens of this country and the crime was committed outside of this country, which means this country cannot claim criminal jurisdiction according to territorial jurisdiction and personal jurisdiction. And in order to protect its national and civil interests, it can claim protective jurisdiction. But the sovereignty of the relative countries is must be taken into consideration, then the double criminality can provide this country with reasonable basis for claiming protective jurisdiction.

of one nation and its citizens are the key factors that determine the content of substantive damage, but the criterion that determines what kinds of specific interests falling into the scope of substantive interests of one nation and its citizens needs to be further researched. However, when computer data or the other related electronic data only passes through one country in transmission, it is not reasonable that this country was considered as having been resulted in substantive damage.[350] The factors can be used to determine substantive damage should include, for example, interests of national defense, and also life right and health right of citizens should be considered into the scope. On the other hand, in the aspect of subjective element, it requires the offenders of cyber transnational organized criminal groups to have actual intention, which means the offenders hope their criminal results and substantive damage occurring in the countries which want to and actually can exercise its criminal jurisdiction. Of course, the standard that how to determine actual intention still need to be farther researched, because actual intention is moral action of the criminals which needs external and objective standards to indentify. These external and objective standards are also guides to establish criterion of determining actual intention.

Once positive conflicts of criminal jurisdiction over CTOC occurred in judicial practice, it means more than one country claim jurisdiction over such crimes, under such condition, connected principle in accordance to substantive damage is a better way to determine which country can and is more reasonable to exercise jurisdiction over this crime. At least, it provides us with a way in the aspect of reducing positive conflicts of jurisdiction over CTOC, since it can exclude the jurisdiction of some countries which do not suffer substantive damage from the related CTOC, just internet signals or data related to this crime pass or arrival at these countries.

[350] The Jurisdiction clause laid down in West Virginia criminal code like this.

2.3 Application in judicial practices

Actually, connected principle in accordance to substantive damage is already a theory that has been accepted by many Chinese scholars. However, whether it can be applied at the level of international community, which depends on if it can be accepted by the international community. However, this principle can be applied in accordance with the following proposition: Firstly, prerequisite is that establishing international judicial assistance in the aspect of criminal jurisdiction about cybercrimes and cyber transnational organized crimes, which will provide a negotiable platform for solving positive conflicts jurisdiction; Secondly, according to connected principle in accordance to substantive damage, if only one country suffer damage from CTOC, it is easy to determine that this victimized country should exercise criminal jurisdiction about this crime; Thirdly, once more than one countries are victims of CTOC, which are more complicated than only one victimized country is involved. Under this situation, it is not enough to determine the criminal jurisdiction just according to connected principle in accordance to substantive damage, how to determine the final jurisdiction still need the help of international judicial assistance agreements. The specific steps are: The first step is that, identifying which countries are victims that suffered substantive damage from certain CTOC. On the basis of the work of first step, combined with the existing international judicial assistance in criminal jurisdiction of cybercrimes and cyber transnational organized crimes, by means of negotiation between these victimized countries, finally making a decision that which country should and be suitable for the one which exercises criminal jurisdiction over the CTOC.

3. Resolution to Negative Conflicts of Jurisdiction

The manifestations of negative conflict of jurisdiction concerning CTOC are reflected in two aspects: firstly, no criminal jurisdiction clauses in domestic criminal law, regional and international convention; secondly, no country claims criminal jurisdiction over these crimes.

At the regional and international level, there are no clear and specific criterions to determine criminal jurisdiction concerning CTOC, even the Europe Cybercrime Convention and the UNTOC provide jurisdiction principles, they are not enough to solve the conflicts of jurisdiction over cyber crime and CTOC. The European cybercrime statutes lack specific jurisdiction clauses, because the general jurisdiction provisions only laid down territorial criminal jurisdiction and personal criminal jurisdiction. The article 15 of the United Nations Convention against Transnational Organized Crime stipulates the jurisdiction of TOC,[351] which stipulates territorial criminal jurisdiction, personal criminal jurisdiction and protective criminal jurisdiction. This dissertation holds that the regional and international convention against cyber crime and transnational organized crime should not ignore this problem. At least they should provide some reasonable criterion to solve the conflicts of criminal jurisdiction. For example, the connected principle in accordance to substantive damage or the other reasonable principles should be established as the guides to solve these kinds of conflicts. Of course, it is difficult to reach on an agreement concerning criminal jurisdiction over cyber crime and CTOC at the regional and international level. However, it merits further research to analyze which theory is better to solve criminal jurisdiction conflicts. If there were specific criminal jurisdiction clause provided in the regional and international conventions against CTOC, once positive jurisdiction conflict occurred, the existing jurisdiction clauses can provide resolution to these conflicts, and it will not need to take time and other resources to reach on new agreement on solving particular conflicts between the involved countries.

[351] See The United Nations Convention against Transnational Organized Crime.

At the national level, whether countries will claim criminal jurisdiction to adjudicate will depend on a number of factors, such as the visibility of the crime, the amount of damage, and the specific connection with the country.[352] In some cyber transnational crimes, if the perpetrators commit crimes in a country that is a cybercrime free haven, and if it happens that they are the citizens of this country, a negative jurisdiction conflict may occur. For example, the targeted countries may not claim criminal jurisdiction, because they think that they did not suffer great harm, perhaps they may also think that some other countries will surly claim jurisdiction. Under this condition, the better way is that universality jurisdiction principle about CTOC should be laid down in domestic criminal law. By means of this the chance of negative jurisdiction conflicts would be highly reduced.

Conclusion of Chapter 5

In the context of the internet, conflict of jurisdiction about CTOC is another urgent problem that needs to be coped with by criminal academic community, regional and international community. This chapter mainly focuses on the following topics: which new conjunctive factors are used to determine criminal jurisdiction of CTOC, legislative clauses and other legislations to expand criminal jurisdiction about all types of cybercrimes, positive and negative conflicts of criminal jurisdiction about CTOC, corresponding theories that were proposed to solve these conflicts, and the connected principle in accordance to substantive damage which is advocated by this dissertation. However, it merits further study whether connected principle in accordance with

[352] Susan W. Brenner and Bert-Jaap Koops, Approaches to Jurisdiction Cybercrime, 2004 Journal of High Technology Law, Vol. IV No. 1.2004.

substantive damage can be wide accepted and popularized in regional and international community.

Chapter 6 Solutions for Informatization of Traditional Transnational Organized Crime and Transformation of Cyber Crime into Organized Cyber Crime

The foregoing chapters analyzed the new characters and trends of OC in the internet age, the criminal legislation and adjustment of criminal policy combating cyber transnational organized crime in the internet age, dilemmas of joint crime theory, legislative absences and judiciary obstacles when combating transnational organized crime in the era of internet and theoretical preparations and legislative countermeasures combating transnational organized crime in the internet era. As a conclusion, in order to effectively combat against CTOC, this chapter proposes what we should do at regional and international level. Under such a situation, there are no existing regional and international conventions particularly combating against CTOC, strengthening police service cooperation and judicial cooperation would be a better way for combating this type of crime. A good sign has been given by European Cybercrime Centre at Europol on 29 September 2014, EC3 published the Internet Organized Crime Threat Assessment, which is the first threat assessment about cyber organized crime written by regional organization.[353] Obviously, regional and international communities are realizing the increasing influence of cybercrimes to organized crimes. It identifies the growing commercialization of cybercrime as one of its principle trends. A service-based criminal business model drives innovation and provides access to a wide range of services facilitating cybercrime. As a consequence, traditional organized criminal groups are now able to step into cybercrime by purchasing bespoke skills and tools to support their criminal business.[354] However, this trend has been proposed and emphasized in the chapter 2, namely, informatization of traditional transnational organized crime. The other important trend, transformation of cyber crime into cyber organized crime, has been also identified and underlined by this dissertation. Another significant point, the

[353] On-line resources, retrieved on 6.October.2014 https://www.europol.europa.eu/latest_publications/31.
[354] On-line resources, retrieved on 6.October.2014 https://www.europol.europa.eu/latest_publications/31.

main challenges for law enforcement agencies, is also realized by this report. It also identifies transnational nature of cybercrime, combined with an increasing sophistication of attacks, problem of attribution, abuse of legitimate services, and inadequate legislations.[355]

Section 1 Theoretical preparations for Informatization of Traditional Transnational Organized Crime and Transformation of Cyber Crime into Organized Cyber Crime

A truth has been indicated by the Europol's report of 2011: Threat Assessment on Internet Facilitated Organized Crime, which said that internet technology increasingly facilitates a wide range of serious and organized crime activity as a communication, research, logistics, marketing, recruitment, distribution and monetarisation tool.[356] This is further indicated by the Internet Organized Crime Threat Assessment of 2014: Traditional organized crime groups, including those with a mafia-structure are beginning to use the service-based nature of the cybercrime market to carry out more sophisticated crimes. This trend towards adopting cybercrime features of a more transient, transactional and less structured organizational model may reflect how all serious crime will be organized in the future.[357] These two reports and this dissertation have realized the trend of informatization of traditional transnational organized crime. Another reality is that the contact between different countries is much closer and more frequent, combined with organized crime becomes a supranational problem, it is much more difficult that one individual country copes with the evolution and development of traditional organized crime by itself. In order to response to the trend of informatization of traditional transnational organized crime and transformation of cyber crime into cyber organized

[355] Ibid
[356] Europol's report of 2011: Threat Assessment on Internet Facilitated Organized Crime.
[357] On-line resources, retrieved on 6.October.2014 https://www.europol.europa.eu/latest_publications/31.

crime, the first work is theoretical preparation for further legislations and judicial practices in the future.

1. Theoretical Preparation for Informatization of Traditional Transnational Organized Crime

In accordance with the evolution of traditional organized crimes, criminal theoretical community should take forward-looking attitude when study the changes and dilemmas brought to us by cybercrime, since the scalability of internet and internet-related ICTs would probably re-change these dilemmas in short time. However, this forward-looking attitude must be established on the basis of substantial researching on facts and documents. Some aspects need to be further and emphatically studied by criminal theoretical community: (1) The definition of traditional organized crime should follow its evolution, cyber organized criminal groups are not limited as traditional types, such as mafia-structured, etc. it would be seriously incompatible with the evolution of traditional organized crimes, if criminal theoretical community still define cyber organized crimes and cyber criminal groups according to mafia-types. The suitable definition of CTOC has been proposed in the chapter 1 of this dissertation; (2) The de-hierarchy (non-hierarchical) trend of traditional organized crime in cyberspace. By means of the internet and internet-related ICTs traditional organized crimes and OCGs have manifested the obvious De-hierarchy trend. Theoretical community should pay attention to the dilemmas of joint crime theory which are brought by De-hierarchy trend. Chapter 4 proposes some solutions about these dilemmas. However, these proposals still need to be further studied whether they can be applied in judicial practices; (3) other theoretical dilemmas. The trend of informatization of traditional organized crime will not just pose challenges to theoretical community, it also causes the other theoretical dilemmas, such as the change of related definitions, the de-hierarchy trend of organized

crime, and the dilemmas of joint crime theory. It is necessary to take an open-mind attitude to the existing and potential dilemmas of traditional organized crimes which are resulted from the trend of informatization of traditional organized crime. Researching on concerning dilemmas of the trend of informatization of traditional organized crime would provide legislations and judicial practices with theoretical preparation.

2. Theoretical Preparation for Transformation of Cyber Crime into Cyber Organized Crime

Another obvious and significant trend revealed by this dissertation is transformation of cyber crime into organized cyber crime, i.e., the trend of organized cybercrimes. Under this context, the scope of cybercrimes is relative narrower. Chapter 2 defines them as pure cyber organized crimes, such as hacking, etc., these crimes were committed in cyberspace instead of in real world, and they appear along with the advent of internet and internet-related ICTs. Actually, they are committed by individual cybercriminal at the beginning of internet, gradually, a professional, continuously, evolving, service-based criminal industry drives individual cyber criminals to associate with each other, finally cyber crime and cyber criminals respectively evolve into cyber organized crimes and cyber organized criminal groups. This evolution has been concluded as the trend of cyber organized crime. However, there is one significant difference between cyber organized crime and traditional organized crime, the former does not have the hierarchy structure as the latter having. Typical manifestations of the structure of cyber organized crime have been analyzed in chapter 4, such as network structure and chain structure. Unquestionably, theoretical community should further and deeply study the dilemmas brought by the trend of cyber organized crime: (1) Dissimilation of traditional joint crime theory, the evolutions about the structure of cyber organized crime bring

difficulties that how to accurately identify every member's role in joint crime.[358] Once these problems cannot be solved, it would be difficult to accurately sentence and convict the members of OCGs; (2) Conflicts of criminal jurisdiction about cyber transnational organized crimes, Chapter 5 focuses on analyzing these dilemmas. The over-expansion of jurisdiction has resulted in positive conflicts of criminal jurisdiction, and probably more than one country, as victims or state of the offenders' nationality, would be involved in organized cybercrimes. Accordingly, positive conflicts of criminal jurisdiction would be exacerbated by the trend of cyber organized crime. Scholars and experts should be research on such problems to provide helpful solutions for legislations and judicial practices prevent this trend.

Section 2 Judicial Cooperation against Cyber Transnational Organized Crime

Judicial cooperation is also an important aspect of combating CTOC. Even though many scholars advocate that punitive function is not the most important function of criminal penalty, it is undeniable that it still plays an important role in the basic functions of criminal penalty. Based on this, to somehow extent, CTOC need to be prevented and cracked down. In view of cyber transnational organized crimes are cross-border problems, judicial cooperation is important to combat them. In order to combat against the increasingly serious COTC, judicial cooperation must be strengthened at the regional and international level.

1. Particular Mechanism for Investigating Cyber Transnational Organized Crime

[358] These dilemmas have been analyzed in chapter 4.

Establishing particular mechanism for investigating cyber transnational organized crimes is an important work at the national, regional and international level. In order to improve investigation of cyber transnational organized crimes, the following text discusses establishment of particular investigation agency and strengthening cross-border police service cooperation.

1.1 Establishment of Particular Investigation Agency

Cybercrime evolves on a daily basis - there are always new vulnerabilities, new criminal methods, new environments for offending and new victims, especially the serious and complicated situation emerged due to the combination of cybercrime and transnational organized crime. In order to cope with the former problems and effectively combat all types of cybercrimes, on 11.01.2013 the European Cybercrime Center started to operate,[359] as an affiliate agency of Europol. One of its major works is combating organized criminal group's illegal activities in cyberspace.[360] Just as the director of Europol, Rob Wainwright said:

> The establishment of the European Cybercrime Center will be the landmark development in the EU's fight against cybercrime. I am delighted that the commission has proposed its establishment at Europol. Organized crime groups, terrorist groups and other criminals are quick to exploit the opportunities afforded by developments in technology, and the time is ripe for the authorities to get one step ahead. The EC3 will provide governments, businesses and citizens throughout the Union with the tools to tackle cybercrime. Building on Europol's proven track record and unique expertise in this area, and with the support of the Member States, other EU bodies, international

[359] In the following we call it as EC3.
[360] On-line news, Retrieved on Dec. 2013 from http://www.most.gov.cn/gnwkjdt/201302/t20130226_99787.htm.

partners, and the private sectors, the EC3 will make the EU smarter, faster and stronger in its fight against cybercrime.[361]

The purpose of EC3 strategy and prevention is to make the citizens and businesses of the EU safe through increased insight, knowledge and rising awareness. The EC3 analyses large amount of data from a variety of sources, both crime data and open sources, to understand how cyber criminals, child sex offenders and fraudsters think and operate. What we learn not only helps law enforcement target its operations more effectively, it also informs changes in policy and legislation and, most important of all, the basis for our advice to citizens and businesses on how to protect themselves from online threats.[362] And now the EC3 is leading project 2020, a strategic foresight initiative for the International Cyber Security Protection Alliance (ICSPA) on the future of cybercrime.[363]

The European EC3 provides us with a good example. The other regions can draw on the experience of Europe, even though it is necessary that the Interpol needs to establish such an EC3-like agency, which can only take the responsibility of dealing with cyber transnational organized crime. The establishment of such EC3-like agencies would support member states and the other regional institutions to build operational and analytical capacity for investigation and cooperation with international partners. The basic functions of these types of agencies should be equipped with:

- Operation and coordination. Supporting the investigation of CTOC among Member States, supporting and coordinating joint investigations carried out by more than one member states (such as at the aspects of technical, analytical and forensic expertise), facilitating law enforcement cooperation with partners outside the region and

[361] On-line news, Retrieved on Dec. 2013 from https://www.europol.europa.eu/ec3/joining-forces.
[362] On-line news, Retrieved on Dec. 2013 from https://www.europol.europa.eu/ec3/strategy
[363] Ibid.

coordinating complex transnational cases in close collaboration with regional court of justice and Interpol.

- Data fusion and data processing capabilities. Gathering and processing information on cyber transnational organized crime, scanning all available sources and extracting information that can be used to combat cyber transnational organized crime and monitor internal network security.

- Training. Because of the fast development of combination of transnational organized crime and cybercrime, the criminals of these types of crime usually are good at ICTs. In order to catch up this trend, staff of law enforcement also needs to be equipped with corresponding ICTs. For example, collaborating closely with some certain police colleges to develop training activities and raise awareness on the issue of CTOC, facilitating research and development, ensuing capacity building among law enforcement, judges and prosecutors, and developing forensic tools to help member states to better detect and prosecute cyber transnational organized crime.

- Strategy and policy. Producing threat assessments concerning cyber transnational organized crime, which includes the trends analyses and forecasts as well as the new developments on locomotive ways of cyber transnational organized criminal groups, which is necessary for the policy-making to combat cyber transnational organized crimes.

- The outreach function. This function is helpful for the comprehensive treatment over CTOC. Of course, it is a way that can throughly help the law enforcement system to promote the efficiency of combating CTOC, such as working closely with private sectors, research community, civil society, academic and computer emergency response teams to detect and respond comprehensively to CTOC; alignment of actions with other relevant international partners, for example, working with European Union Cybercrime Taskforce.

1.2 Strengthening Cross-border Police Service Cooperation

This dissertation holds that establishing particular investigation agency at regional and international level is a better way to combat CTOC. However, it is unknown that any region has been provided with qualifications for establishing such agencies. Under the situation that there is no available existing particular investigation agency for combating cyber transnational organized crime, it is necessary to strengthen cross-border police service cooperation. But no nation could apply its criminal laws to conduct occurring within the physical territory of another nation.[364] Under this condition, the bilateral or multilateral agreement concerning police service over cyber transnational organized crime is required between different countries. The contents of such agreement at regional or international level at least should include the following aspects:

- Collaboration with requests for mutual investigating assistance. CTOC usually crosses more than one countries' border, it is insufficient that only by means of the power of a single country to combat CTOC, because investigating such crimes outside the territory of an individual state is beyond the scope of its authority. Collaboration is necessary for investigating such crimes, and the required states should provide the requiring states with corresponding assistance.

- Eliminating obstacles of investigation between different countries. Each individual country has its own legal system, standard of ICTs and language, which usually become the biggest obstacles of investigating CTOC. One of the priorities is that eliminating such obstacles, such as trying to unify the standard of criminalizing illegal cyber transnational organized activities and ICTs, carrying out regular

[364] See, e.g., The Apollon, 22 U.S.(9 Wheat) 362,371(1824). See also United Nations Convention Against Transnational Organized Crime, Article 4("Protection of Sovereignty") (2000), availalbe at http://www.uncjin.org/Doucuments/Conventions/dcatoc/final_documents_2/convention_eng.pdf. See generally RESTATEMENT(THIRD) OF FOREIGN RELATIONS LAW OF THE UNITED STATES § 206 cmt. b (1987).

language training and legal knowledge of member states among the staff of law enforcements between state parties.

- Unified investigation over specific case. Since one specific CTOC often crosses more than one country, such bilateral or multilateral agreements should law down provisions about unified investigation over specific CTOC. Unified investigation can largely enhance the efficiency of combating such crime.

- Strengthening the rate of reaction to CTOC and reinforcing collection and preservation of evidence. Since CTOC usually has instantaneous character and rapidity, the evidences of such crimes are often difficult to preserve, the corresponding bilateral and multilateral agreements need to law down provisions concerning this aspects of works. And in order to strengthen this kind of work, some certain special investigative means need to be used, such as electronic monitoring with ICTs, etc.

- Each state party should collects, exchanges and analyzes documents over cyber transnational organized crime. Collecting, exchanging and analyzing the documents over CTOC is helpful for prosecution, punishment and prevention of such crimes.

- Emphasizing early proactive warning against cyber transnational organized crime. The majority of CTOC has character of serious harmfulness, so the member states of such agreements should pay more power to early proactive warning to against such crimes, for example, regularly monitoring illegal activities of OCGs.

2. Signing and Ratification of Concerning Regional and International Agreements

It is necessary that signing and ratification of concerning regional and international agreements, which can provide the whole detailed work of combating cyber

transnational organized crime with legal frameworks. And combating CTOC needs collaboration between all involved countries. However, as the first step to against CTOC, how to sign and ratify concerning regional and international agreements merits farther research. Of course, after the member states signed and ratified these concerning agreements, in accordance with them related authorities must legislate or amend domestic laws to get rid of barriers of judicial collaboration against CTOC, and on the base of this they should continually improve specific procedure and measure of judicial cooperation at region and international level. The major provisions should be laid down in these agreements as follows:

- Unified standard of criminal jurisdiction over cyber transnational organized crime. Since increasingly positive and negative criminal jurisdiction conflicts over cybercrime is becoming more serious than before,[365] both of them would create big obstacle for combating cybercrime.[366] Once there is jurisdiction conflict over a specific case of CTOC, and all the involved parties cannot reach an agreement concerning which party should exercise jurisdiction, the related provisions should provide a guide that how to solve these conflicts. For instance, the involved parties can depute the jurisdiction conflicts to some certain agencies to solve it, and these agencies have the power of giving final approval over this jurisdiction conflicts.

- Unified criteria of collecting and taking digital evidences. Prosecution and trail of CTOC usually involve taking digital evidences, but as the matter of fact, there are no unified criteria concerning collecting and taking digital evidences of CTOC at regional and international level. Accordingly, this absence has largely weakened the work of combating CTOC. In views of this situation, it is necessary to stipulate the provisions about unified criteria of collecting and taking digital evidences in such regional and international agreements.

[365] Yu Zhigang, The Age of Informationalized Transnational Crime and Chinese Choice concerning The Council of Europe Convention on Cybercrime. Legal Forum, Issue 2, 2013.
[366] This dissertation holds an opinion that cyber transnational organized crime falls into the scope of cyber crime.

- Provisions concerning regular training which equip prosecutors and judges with necessary knowledge and technique about cyber transnational organized crime. The complex characters of CTOC require prosecutors and judges to grasp corresponding knowledge and technique about CTOC.

- Establishment of coordination agency for judicial cooperation. These regional and international agreements should lay down provisions about establishing coordination agency for judicial cooperation when there is sufficient condition at suitable time.

- Simplifying procedure of transferring evidence and extraditing criminals of cyber transnational organized crime. On the one hand, digital evidences of CTOC are more difficult to be collected and saved than transnational organized crime in real world, in order to enhance the efficiency of combating such crimes, it is necessary to lay down this kind of provisions. On the other hand, simplifying procedure of extraditing suspects and criminals of CTOC is also important for combating these crimes. This kind of provisions can refer to the existing provisions concerning extraditing criminals of transnational organized crime in real world.[367]

3. Establishment of Coordination Agency for Judicial Cooperation

At the regional and international level, with some certain conditions at proper time, for example, some individual countries can propose to establish coordination agency for judicial cooperation for combating the serious CTOC, theses countries should embark on preparation work of establishing this type of agency. The major reason is that many problems in judicial cooperation are caused by the misunderstanding due to the differences of different law systems. Establishment of such agencies can largely

[367] This dissertation holds an opinion that there is no difference concerning extraditing provisions between cyber transnational organized crime and transnational organized crime occurring in real world.

enhance the efficiency of combating CTOC. The main function of these agencies should include:

- Coordinating jurisdiction conflicts. In view of almost all countries are expanding their criminal jurisdiction over cybercrime,[368] once two countries or more than two countries claimed jurisdiction over one CTOC at the same time, and they could not come to an agreement about this dispute. Under this situation a coordinating agency is necessary to solve this problem. The disputed parties can submit this jurisdiction conflict to such a coordinating agency, which has the power of giving final approval over jurisdiction conflicts according to the regional or international agreements about judicial cooperation, and this final verdict has binding force to the disputed parties.

- Coordinating disagreements during the process of judicial cooperation concerning cyber transnational organized crime. During the process of regional and international judicial cooperation, all kinds of difficulties can be confronted by the parties of cooperation. Such difficulties may come from exchanging information of specific CTOC, transferring digital evidences and extraditing suspects or criminals. These coordination agencies are established on the agreement of all parties, so it plays a neutral role in the process of coordinating and solving these problems, and usually the disputed parties should accept the final solutions.

- Establishing database about cyber transnational organized crime. These coordinating agencies should establish database about CTOC. This database should basically include statistics from the member states, such as decided cases, pending litigation and cases that did not enter the trial. Base on these statistics, the agencies can analyze the trends of CTOC, which is significant for the prevention of CTOC.

[368] Yu Zhigang, The Age of Informationalized Transnational Crime and Chinese Choice concerning The Council of Europe Convention on Cybercrime. Legal Forum, Issue 2, 2013

Conclusion of Chapter 6

This chapter focuses on the solutions for informatization of traditional transnational organized crime and transformation of cyber crime into cyber organized crime. The corresponding solutions are discussed from two aspects: One is the theoretical preparations for informatization of traditional transnational organized crime and transformation of cyber crime into cyber organized crime; another is judicial cooperation against cyber transnational organized crime. The first aspect concludes the problems that have been analyzed and discussed in the above chapters. The seconds aspects mainly proposes the following solutions, which include the establishment of particular investigation agency, strengthening cross-border police service cooperation, signing and ratification of concerning regional and international agreements and establishment of coordination agency for judicial cooperation. To be frank, these solutions are just proposals for combating against transnational organized crime in the context of the internet. However, regional and international judicial cooperation are significant for preventing and keeping cyber transnational organized crimes away from our civil society.

Conclusion of This Dissertation

The interaction and integration between transnational organized crime and cybercrime create cyber transnational organized crime, which makes the situation even worse and the work of combating transnational organized crime and cyber crime much difficult than before. In view of this authorities of every country must take countermeasures to against it. This dissertation takes an abroad viewpoint to analyze this criminal phenomenon, in order to indicate the trend of organized crime in the context of the internet, 250 cases from May of 2003 to July of 2013 concerning organized crime connected with the internet or ICTs have been analyzed. Through case study one important obvious trend is indicated that organized crime is developing into cyber transnational organized crime. The combination of OC and ICTs brought us some complicated problems. The prominent problems include criminal jurisdiction conflicts and the dilemmas of joint crime theory. Furthermore, what kind of countermeasures should be taken to combat CTOC was discussed in the following. Of course, to some extent these proposals are just preparatory and raw outline, the details of them merit farther study. Because CTOC is not only business of individual country, it has become a supranational problem, and these countermeasures usually need to be implemented cross multiple countries, so the details of countermeasures that can be accepted by majority of sovereign nations need to be farther studied, especially those countermeasure would be carried out at regional or international level. It can be imagined that the process of negotiation would be difficult and time-consuming, but in order to combat cyber transnational organized crime, we must move on.

Bibliography

1. Howard Abadinsky, (1990), Organized Crime (Third Edition), Nelson-Hall Inc.

2. Jay S. Albanese and Dilip K. Das,(2003), In Jay S. Albanese , Dilip K. Das and Arvind Verma. (eds). (2003), *Organized Crime: World Perspective*, Pearson Education, Inc., Upper Saddle River, New Jersey 07458.

3. See, e.g., The Apollon, 22 U.S. (9 Wheat) 362,371(1824). See also United Nations Convention against Transnational Organized Crime, Article 4("Protection of Sovereignty") (2000), available at http://www.uncjin.org/Doucuments/Conventions/dcatoc/final_documents_2/convention_eng.pdf. See generally RESTATEMENT(THIRD) OF FOREIGN RELATIONS LAW OF THE UNITED STATES § 206 cmt. b (1987).

4. Francesc. Balazuo. Italian Legislation on Organized Crime. Juvenile Deliquency Research. Issue 5-6 (1997).

5. M.Cherif Bassiouni and Eduardo Vetere, (1998), Towards Understanding Organized Crime and Its Transnational Manifestations, M.Cherif Bassiouni and Eduardo Vetere, (eds), In *Organized Crime: A Compilation of U.N. Documents 1975-1998*, Transnational Publishers, Inc.

6. Susan W. Brenner and Bert-Jaap Koops ,Approaches to Jurisdiction Cybercrime, 2004 Journal of High Technology Law, Vol. IV No. 1.2004.

7. John Broome, (2003), In Jay S. Albanese, Dilip K. Das and Arvind Verma. (eds). (2003), *Organized Crime: World Perspective*, Pearson Education, Inc., Upper Saddle River, New Jersey 07458.

8. John Broome, Organized Crime: An Australian Perspective, In *Organized Crime: a World Perspective*, Third International Police Executive Symposium, Kanagawa University, Yokohama, Japan Nov 28-Dec 1, 1996, The Society of Law, University of Kanagawa, Vol.31, No. 3, 1997.

9. Chen Qi, Research on the Jurisdiction Problem of Online Tort Disputes, Journal of Jimei University, Philosophy and Social Sciences Edition, 2006, Issue 1.

10. Chimel v. California, 395 U.S.752 (1969), see in Robert W. Taylor, et al, (2006), *Digital crime and digital terrorism*, Pearson Education, Inc., Upper Saddle River, New Jersey.

11. Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA, Official Journal of the European Union, 14.Augest.2013.

12. Maximilian Edelbacher, Organized Crime in Austtria-Vienna: The Gateway to the East, In *Organized Crime: A World Perspective*, Third International Police Executive Symposium, Kanagawa University, Yokohama, Japan Nov 28-Dec 1, 1996, The Society of Law, University of Kanagawa, Vol.31, No. 3, 1997.

13. Maximilian Edelbacher, Organized Crime: An Austrian Perspective, I N S. Einstein

and M. Amir (ed.) (1999), *Organized Crime: Uncertainties and Dilemmas*, the Office of International Criminal Justice, the University of Illionis at Chicago.

14. Cyrille Fijnaut and Letizia Paoli, The Initiatives of the European Union and the Council of Europe, In Cyrille Fijnaut and Letizia Paoli (ed.) (2004), *Organized Crime in Europe: Concepts Patterns and Control Policies in the European Union and Beyond*, Springer.

15. Feng Chaohui and Huang Qingsheng, Comparison of Anti-cyber Crime Law between Different Countries, Network Security Technology and Application,(02.2006).

16. Gianluca Fulvetti, The Maifa and the " Problem of the Mafia": Organized Crime in Italy, 1820-1970, In Cyrille Fijnaut and Letizia Paoli (ed.) (2004), *Organized Crime in Europe: Concepts Patterns and Control Policies in the European Union and Beyond*, Springer.

17. Yakov Gilinskiy and Yakov Kostjukovsky, From Thievish Artel to Criminal Corporation: the History of Organized Crime in Russia, In Cyrille Fijnaut and Letizia Paoli (ed.) (2004), *Organized Crime in Europe: Concepts Patterns and Control Policies in the European Union and Beyond*, Springer.

18. Gong Yanmei, Network Crime Jurisdiction Conflicts and Determine, Master dissertation, published by Lanzhou University, 2012.

19. Sean Grennan and Marjie T. Britz, *Organized Crime: a Worldwide Perspective*,

Pearson Education, Inc., Upper Saddle River, New Jersey, 2006.

20. Gu Wenling, Research on European Organized Crime, East China University of Politics and Law, issued on 18.April.203.

21. Han Zhe, the Substantive Characteristics and Criminal Jurisdiction of Cybercrime, Journal of Shandong Police College, Issue 3. 2003.

22. He Bingsong, Organized Crime and Its Containment in China, In *Organized Crime: A World Perspective*, Third International Police Executive Symposium, Kanagawa University, Yokohama, Japan Nov 28-Dec 1, 1996, The Society of Law, University of Kanagawa, Vol.31, No. 3, 1997.

23. Arizona v. Hicks, 480 U.S. 321 (1987), see in Robert W. Taylor, et al, (2006), *Digital crime and digital terrorism*, Pearson Education, Inc., Upper Saddle River, New Jersey.

24. Hiller, Janine S. and Ronnie Cohen. Internet Law and Policy, Upper Saddle River, NJ: Prentice Hall, 2002.

25. Daniel J. Koenig, (1996), Follow the Money Enterprise Crime in Canada, (p.208), In *Organized Crime: a World Perspective*, Third International Police Executive Symposium, Kanagawa University, Yokohama, Japan Nov 28-Dec 1, 1996, The Society of Law, University of Kanagawa, Vol.31, No. 3, 1997.

26. Wayne R. LaFave, SUBSTANTIVE CRIMINAL LAW § 4.3(e) (2003). See Susan

W. Brenner and Bert-Jaap Koops, Approaches to Jurisdiction Cybercrime, 2004 Journal of High Technology Law, Vol. IV No. 1.2004.

27. Katrin Lange, Many a Lord is Guilty, Indeed For Many a Poor Man's Dishonest Deed: Gangs of Robbers in Early Modern Germany, In Cyrille Fijnaut and Letizia Paoli (ed.) (2004), *Organized Crime in Europe: Concepts Patterns and Control Policies in the European Union and Beyond*, Springer.

28. Liu Shoufen and Fang Shuxin. Analyzing Eight Countries' Legislation against Cyber Crime and their Enlightenment to the Legislation of China, Law Science Magzine, Volume 25, (15.09.2004).

29. Liu Wei, Introduction of Foreign Prevention and Control System of Cyber Crime, Netinfo Security, Issue 6 (2005).

30. Liu Xiaoli and Zhang Liyun, Overview of U.S. Computer Crime Legislation, Network Security Technology and Application, Issue 8 (2007).

31. Lu Jianping eds. *Comparative Study of Organized Crime*. Law Press China, 2004.

32. Hiroyuki Matsumoto eds. *Internet, Information Society and Law-the German and Japanese Symposium,* cited in Zheng Shanzhe, Cybercrime and the Principle of Territorial Criminal Jurisdiction, Chinese Journal of Law, 2006, issued 5.

33. Letizia Paoli and Cyrille Fijnaut (2004), In Cyrille Fijnaut and Letizia Paoli (ed.) (2004), *Organized Crime in Europe: Concepts Patterns and Control Policies in the*

European Union and Beyond, Springer.

34. Pi Yong, the German Cyber Crime Legislation under the Background of Integration of European Criminal Law. Peking University Law Journal, Vol.23，No.5 (2011).

35. Qu Xinjiu eds. *Science of Criminal Law*, China University of Political Science and Law Press, issued 2008. P.18.

36. Leonardo Jesus Ramirez Rirea, et.al, (2003), In Jay S. Albanese, Dilip K. Das and Arvind Verma. (eds). (2003), *Organized Crime: World Perspective*, Pearson Education, Inc., Upper Saddle River, New Jersey 07458.

37. Allexander Seger, (2012), Cyber Crime and Economic Crime, Maximillian Edelbacher, Peter Kratcoski and Michael Theil (ed), *Financial Crimes: A Threat to Global Security*, CRC Press.

38. Harald Otto Schweizer, et.al, Organized Crime: A U.S. Perspective. In Jay S. Albanese , Dilip K. Das and Arvind Verma. (eds). (2003) *Organized Crime: World Perspective*, Pearson Education, Inc., Upper Saddle River, New Jersey 07458.

39. Ulrich. Sieber, the Threat of Cybercrime in Organized Crime in Europe: The Threat of Cybercrime Situation Report 2004, Council of Europe Publishing 2005.

40. Antonio La Spina, The Paradox of Effectiveness: Growth, Institutionalisation and Evaluation of Anti-Mafia Policies in Italy, In Cyrille Fijnaut and Letizia Paoli (ed.) (2004), *Organized Crime in Europe: Concepts Patterns and Control Policies in the*

European Union and Beyond, Springer.

41. supra § II. See also Restatement (Third) of Foreign Relations Law of the United States § 404 (1987) ("A state has jurisdiction to define and prescribe punishment for certain offenses recognized by the community of nations as of universal concern, such as piracy, slave trade, attacks on or hijacking of aircraft, genocide, war crimes, and perhaps certain acts of terrorism, even where none of the bases of jurisdiction indicated in § 402 is present"). Cf. United States v. Yousef, 327 F.3d 56, 99-100 (2d Cir. 2003) (district court improperly found it could exercise universal jurisdiction over terrorist activities). See in Susan W. Brenner and Bert-Jaap Koops ,Approaches to Jurisdiction Cybercrime, 2004 Journal of High Technology Law, Vol. IV No. 1.2004.

42. Robert W. Taylor, et al, (2006), *Digital crime and digital terrorism*, Pearson Education, Inc., Upper Saddle River, New Jersey.

43. U.S. Department of Justice. Searching and Seizing Computer and Obtaining Electronic Evidence in Criminal Investigations （Washington, DC: U.S. Department of Justice, 2002.

44. Arvind Verma, (1997), Organized Crime in India, In *Organized Crime: A World Perspective*, Third International Police Executive Symposium, Kanagawa University, Yokohama, Japan Nov 28-Dec 1, 1996, The Society of Law, University of Kanagawa, Vol.31, No. 3, 1997.

45. Wang Li, Monographic Study of Organized Crime, People's Press, p.17.

46. Wang Shuai, Jurisdiction about Cyber-crime, Master dissertation, published by Liaoning University, 2012.

47. Xu Jieqing, (2006), *a Study of Organized Crime in Taiwan District and the Coutermesasures*, Chiense Procuratorial Press.

48. Xu Kai. (2011). the Characteristics of Organized Criminals of Russian in 21C, Journal of Heilongjiang Administrative Cadre Institute of Politics and Law, Sum No.93.

49. Xupan, (24, Aug 2012). The police of Philippine uncovered a fraud gang of China. Global Times, p.03.

50. Yang Caixia, The Enlightenment of International Anti-cybercrime Legislation to China—Taking the Council of Europe Convention on Cybercrime as the Focus, Present Day Law Science, Issue 3, 2008.

51. Yang Jianzheng, the Legislation of Computer Law Worldwide, Journal of Zhengzhou University, Issue 5 (1999).

52. Yu Zhigang, *Research on the Dissimilation of Traditional Crime in the Internet Age*, China Procuratorial Press, 2010.

53. Yu Zhigang, The Age of Informationalized Transnational Crime and Chinese

Choice concerning The Council of Europe Convention on Cybercrime. Legal Forum, Issue 2, 2013.

54. Zhao Bingzhi and Zhang Xinping, attempted to Research on Cyber Joint Crime, issued by Tribune of Political Science and Law, No 5 of 2002.

55. Zhao Chi, the Investigation of British Legislation against Organized Crime, International Research, Issue 403 (2013).

56. 8 terrorists are wanted by the Ministry of Public Security of the People's Republic of China. Yangzhou Times, (22, Oct 2008), p.A10.

Internet sources

1. Mike Faure, Russia joining hand with the United States fighting against Maf ia. Message posted to http://news.fm365.com/guoji/20000921/145932.htm.

2. On-line news, Retrieved on 06.Oct.2013 from http://www.bmi.gv.at/cms/BK/p ublikationen/Cybercrime.aspx.

3. On-line news, Retrieved on 06.Oct.2013 from http://www.bmi.gv.at/cms/BK/p ublikationen/krim_statistik/Statistiken_2011.aspx.

4. On-line news, Retrieved on 06.Oct.2013 from http://www.bmi.gv.at/cms/BK/p ublikationen/krim_statistik/Statistiken_2012.aspx.

5. On-line news, Retrieved on 06.Oct.2013 from http://www.bmi.gv.at/cms/BK/publikationen/krim_statistik/Statistiken_2013.aspx.

6. On-line news, Retrieved on 09.Oct.2013 from http://www.fbi.gov/stats-services/publications/2011-national-gang-threat-assessment.

7. On-line news, Retrieved on 12.Oct.2013 from https://www.europol.europa.eu/content/publication/iocta-threat-assessment-internet-facilitated-organised-crime-1455.

8. On-line news, Retrieved on 16.Oct.2013 from https://www.europol.europa.eu/content/eu-serious-and-organised-crime-threat-assessment-socta.

9. On-line news, Retrieved on 16.Oct.2013 from http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm.

10. The United Nations Convention against Transnational Organized Crime, Retrieved on 26 July 2013 from https://www.unodc.org/unodc/en/treaties/CTOC/index.html?ref=menuside.

11. Susanne Reinde-Krauskopf and Farsam Salimi, Retrieved on 01.August.08 from http: //www.parlament.gv.at/PAKT/VHG/XXIV/III/III OO348/fname 263545.pdf.

12. On-line resources, retrieved on 6. Aug. 2014 from http://www.organized-crime.de/OCLAWS.htm.

13. On-line resources, retrieved on 07.Aug.2014 from http://www.cybercrimelaw.net/US.htm.

14. On-line resources, retrieved on 08. Aug. 2014 from http://www.cybercrimelaw.net/Italy.html.

15. On-line resources, retrieved on 09.Aug.2014 from http://www.cybercrimelaw.net/Germany.html.

16. On-line resources, retrieved on 10.Aug.2014 from http://www.ris.bka.gv.at/Ergebnis.wxe?Suchworte=datenschutzgesetz+51&Abfrage=Gesamtabfrage&x=10&y=7.

17. On-line resources, retrieved on 10.Aug.2014 from http://www.cybercrimelaw.net/France.html.

18. On-line resources, retrieved on 22.Aug.2014 from http://www.cybercrimelaw.net/UK.html.

19. On-line resources, retrieved on 22.Aug.2014 from http://www.cybercrimelaw.net/Japan.html.

20. On-line resources, retrieved on 22.Aug.2014 from http://www.cybercrimelaw.net/Japan.html.

21. On-line news, retrieved on 10.Sep.2014 from http://news.qq.com/a/20051214/000497.htm.

22. On-line resources, retrieved on 10.Sep.2014 from http://www.ris.bka.gv.at/Bundesrecht/.

23. On-line news, retrieved on 16.september.2014 from http://www.chinanews.com/gn/news/2007/12-25/1114636.shtml.

24. On-line news, retrieved on 16.september.2014 from http://www.docin.com/p-771707862.html.

25. On-line news, retrieved on 16.september.2014 from http://www.mps.gov.cn/n16/n1252/n1687/n2272/3414264.html.

26. On-line news, retrieved on 16.september.2014 from http://www.mps.gov.cn/n16/n1252/n1762/n2452/2580402.html.

27. On-line news, retrieved on 28.Apr.2014 from http://www.mps.gov.cn/n16/n1237/n2131945/3435067.html.

28. On-line news, retrieved on 20. August.2014 from http://www.mps.gov.cn/n16/n1252/n1762/n2452/2461405.html.

29. On-line news, Retrieved on 28. Apr. 2014 from http://tech.sina.com.cn/roll/2008-12-07/1706902529.shtml.

30. Qu Xuewu, on-line article, retrieved on 29.Apr.2014 from http://www.chinalawedu.com/news/16900/173/2004/9/re55364858341419400221750_132125.htm..

31. On-line resources, retrieved on 6.October.2014 https://www.europol.europa.eu/latest_publications/31.

32. On-line resources, retrieved on 6.October.2014 https://www.europol.europa.eu/latest_publications/31.

33. On-line resources, retrieved on 6.October.2014 https://www.europol.europa.eu/latest_publications/31.

34. On-line news (2013). Retrieved on 30.Mar.2013 from http://www.mps.gov.cn/.

35. Cybercrime: A Global Growing Problem. Retrieved on 03.Aug.2013 from https://www.europol.europa.eu/ec/cybercrime-growing.

36. See the Criminal Development of Austria between 2004 and 2013 and the Cybercrime Report of Austria of 2011 and 2012. Retrieved on 28.Dec.2013 from http://www.bmi.gv.at/cms/BK/meldestellen/internetkrimina/start.aspx.

37. On-line news (2013). Retrieved on 01. Sept.2013 from http://www.interpol.int/Crime-areas/Cybercrime/Cybercrime.

38. On-line news (2013). Retrieved on 28. Aug.2013 from http://www.fbi.gov/.

39. On-line news (2013). Retrieved on 01. Sept.2013 from http://www.law.cornell.edu/uscode/text/18/1961.

40. On-line article (2013). The General Situation of Legislation of Macau against Organized Crime. Retrieved on 10.Sept.2013 from http://www.chinalawedu.com/new/201211/wangying201211162030424504626 4.shtml.

41. Cui Man, Research on the Organized Crime in Russia, On-line dissertation. Retrieved on 15.Sept.2013 from http://epub.cnki.net/kns/detail/detail.aspx?QueryID=3&CurRec=1&recid=&FileName=2009087424.nh&DbName=CDFD0911&DbCode=CDFD&pr=.

42. On-line article (2013). Retrieved on 19.Sept.2013 from http://www.unodc.org/unodc/en/organized-crime/emerging-crimes.html.

43. On-line news. Retrieved on 05.Oct.2013 from http://baike.baidu.com/link?url=o9ivyKBtBAXCevBDiYxe3s3VRaptrFPNScUbSmjlhAwgwEQC57qmeZvhgYGbPBe6.

44. Judgment of the Munich Court in the "CompuServe Case" (Somm Case), on-line news. Retrieved on 26.Oct.2013 from http://www.kuner.com/data/reg/somm.html.

45. Wang Minghao, on-line hacker school was dismantled by the Police of Xucang of Henan Province. On-line news. Retrieved on 27.Oct.2013 from http://www.people.com.cn/GB/paper464/16946/1488486.html.

46. On-line news. Retrieved on 27.Oct.2013 from http://www.mps.gov.cn/n16/n1252/n1762/n2452/2461405.html.

47. On-line news. Retrieved on 01.Dec.2013 from http://www.most.gov.cn/gnwkjdt/201302/t20130226_99787.htm.

48. On-line news. Retrieved on 02.Dec.2013 from https://www.europol.europa.eu/ec3/joining-forces.

49. On-line news. Retrieved on 02.Dec.2013 from https://www.europol.europa.eu/ec3/strategy.

50. On-line news. Retrieved on 30.July.2013 from http://www.mps.gov.cn/ http://www.soca.gov.uk/news/552-eleven-arrests-as-global-investigation-dismantles-criminal-web-forum.

51. On-line news. Retrieved on 30.July.2013 from http://www.soca.gov.uk/news/551-money-laundering-network-jailed-.

52. On-line news. Retrieved on 30.July.2013 from http://www.soca.gov.uk/news/543-judge-jails-international-cocaine-trafficker.

53. On-line news. Retrieved on 30.July.2013 from http://www.soca.gov.uk/news/539-carbon-credit-thieves-jailed.

54. On-line news. Retrieved on 30.July.2013 from http://www.soca.gov.uk/news/533-websites-trading-in-stolen-bank-data-targeted.

55. On-line news. Retrieved on 30.July.2013 from http://www.rcmp-grc.gc.ca/news-nouvelles/2013/06-27-pangea-eng.htm.

56. On-line news. Retrieved on 30.July.2013 from http://www.afp.gov.au/media-centre/news/afp/2013/march/federal-and-state-law-enforcement-partnership-dismantles-international.

57. On-line news. Retrieved on 30.July.2013 from http://www.afp.gov.au/media-centre/news/afp/2013/march/117kg-of-drugs-seized-in-organised-crime-investigation-spanning-five-countries.

58. On-line news. Retrieved on 30.July.2013 from http://www.afp.gov.au/media-centre/news/afp/2013/march/117kg-of-drugs-seized-in-organised-crime-investigation-spanning-five-countries.

59. On-line news. Retrieved on 30.July.2013 from http://www.interpol.int/News-and-media/News-media-releases/2013/N20130619.

60. On-line news. Retrieved on 30.July.2013 from http://www.interpol.int/News-and-media/News-media-releases/2013/PR079.

61. On-line news. Retrieved on 30.June.2013 from http://www.fbi.gov/losangeles/press-releases/2012/armenian-power-member-and-three-armenian-power-associates-convicted-in-los-angeles-for-roles-in-identity-theft-ring.

62. On-line news. Retrieved on 30.June.2013 from http://www.fbi.gov/news/stories/2012/march/predators_030112/predators_030112.

63. On-line news. Retrieved on 30.June.2013 from http://www.fbi.gov/newhaven/press-releases/2012/alleged-organized-crime-associates-among-20-charged-with-operating-illegal-gambling-businesses-in-connecticut.

64. On-line news. Retrieved on 30.June.2013 from http://www.fbi.gov/news/stories/2012/april/grandparent_040212/grandparent_040212.

65. On-line news. Retrieved on 30.June.2013 from http://www.mps.gov.cn/n16/n1252/n1762/n2452/3179808.html.

66. On-line news. Retrieved on 30.June.2013 from http://www.mps.gov.cn/n16/n1252/n1762/n2452/3147324.html.

67. On-line news. Retrieved on 30.June.2013 from http://www.mps.gov.cn/n16/n1237/n1342/n803715/3296069.html.

68. On-line news. Retrieved on 30.June.2013 from http://www.mps.gov.cn/n16/n1237/n1342/n803715/3330551.html.

69. On-line news. Retrieved on 30.June.2013 from http://www.mps.gov.cn/n16/n1237/n1342/n803715/3393152.html.

70. On-line news. Retrieved on 30.June.2013 from http://www.mps.gov.cn/n16/n1237/n1342/n803715/3617482.html.

71. On-line news. Retrieved on 30.June.2013 from http://www.mps.gov.cn/n16/n1252/n1687/n2227/3414318.html.

72. On-line news. Retrieved on 30.June.2013 from http://www.soca.gov.uk/news/453-worldwide-arrests-of-online-carding-forum-users-.

73. On-line news. Retrieved on 30.June.2013 from http://www.soca.gov.uk/news/446-web-domains-seized-in-international-operation-to-target-online-fraudsters.

74. On-line news. Retrieved on 30.June.2013 from http://www.afp.gov.au/media-centre/news/afp/2012/november/seven-arrested-in-australias-largest-credit-card-data-theft-investigation.

75. On-line news. Retrieved on 30.June.2013 from http://www.afp.gov.au/media-centre/news/afp/2012/january/Media%20Release%20-%20%20Joint%20agency%20investigation%20dismantles%20organised%20crime%20syndicate.

76. On-line news. Retrieved on 30.June.2013 from http://www.afp.gov.au/media-centre/news/afp/2012/september/further-arrests-laid-in-multimillion-dollar-identity-crime-syndicate-investigation.

77. On-line news. Retrieved on 30.June.2013 from http://www.cisaw.cn/html/jishuyuandi/552.html.

78. On-line news. Retrieved on 29.May.2013 from http://www.fbi.gov/news/stories/2011/june/cyber_062211/cyber_062211.

79. On-line news. Retrieved on 29.May.2013 from http://www.fbi.gov/news/stories /2011/november/malware_110911/malware_110911.

80. On-line news. Retrieved on 29.May.2013 from http://www.fbi.gov/news/stories /2011/april/botnet_041411.

81. On-line news. Retrieved on 29.May.2013 from http://www.fbi.gov/newyork/press-releases/2011/leader-of-armenian-organized-crime-ring-pleads-guilty-in-manhattan-federal-court-to-racketeering.

82. On-line news. Retrieved on 29.May.2013 from http://www.fbi.gov/newyork/press-releases/2011/manhattan-u.s.-attorney-charges-26-gambino-crime-family-leaders-members-and-associates-on-racketeering-murder-narcotics-firearms-and-other-charges.

83. On-line news. Retrieved on 29.May.2013 from http://www.fbi.gov/philadelphia /press-releases/2011/leadership-members-and-associates-of-the-philadelphia-la-cosa-nostra-family-charged-with-racketeering-conspiracy-and-related-crimes.

84. On-line news. Retrieved on 29.May.2013 from http://www.fbi.gov/newyork/press-releases/2011/91-leaders-members-and-associates-of-la-cosa-nostra-families-in-four-districts-charged-with-racketeering-and-related-crimes-including-murder-and-extortion.

85. On-line news. Retrieved on 29.May.2013 from http://www.fbi.gov/news/stories /2011/october/gangs_102011/gangs_102011.

86. On-line news. Retrieved on 29.May.2013 from http://www.soca.gov.uk/news/3 64-smart-phone-malware-highlighted-by-get-safe-online-week-.

87. On-line news. Retrieved on 29.May.2013 from http://www.afp.gov.au/media-c entre/news/afp/2011/november/identity-crime-raids-seize-10000-fake-credit-three -arrested.

88. On-line news. Retrieved on 29.May.2013 from http://www.interpol.int/News-a nd-media/News-media-releases/2011/N20110117.

89. On-line news. Retrieved on 29.May.2013 from http://www.mps.gov.cn/n16/n1 252/n1687/n2272/3414264.html.

90. On-line news. Retrieved on 16.Apr.2013 from http://www.fbi.gov/newyork/pre ss-releases/2010/nyfo042010.htm.

91. On-line news. Retrieved on 16.Apr.2013 from http://www.fbi.gov/news/stories/ 2010/october/cyber-banking-fraud/cyber-banking-fraud.

92. On-line news. Retrieved on 16.Apr.2013 from http://www.mps.gov.cn/n16/n1252/n1762/n2452/2634542.html.

93. On-line news. Retrieved on 16.Apr.2013 from http://www.mps.gov.cn/n16/n1252/n1762/n2452/2580402.html.

94. On-line news. Retrieved on 16.Apr.2013 from http://www.mps.gov.cn/n16/n1252/n1762/n2452/2562633.html.

95. On-line news. Retrieved on 16.Apr.2013 from http://www.mps.gov.cn/n16/n1252/n1762/n2452/2461405.html.

96. On-line news. Retrieved on 16.Apr.2013 from http://www.mps.gov.cn/n16/n1252/n1762/n2452/2455898.html.

97. On-line news. Retrieved on 16.Apr.2013 from http://www.mps.gov.cn/n16/n1252/n1762/n2452/2442526.html.

98. On-line news. Retrieved on 16.Apr.2013 from http://www.mps.gov.cn/n16/n1252/n1762/n2452/2442544.html.

99. On-line news. Retrieved on 16.Apr.2013 from http://www.mps.gov.cn/n16/n1252/n1762/n2452/2441268.html.

100. On-line news. Retrieved on 16.Apr.2013 from http://www.mps.gov.cn/n16/n1252/n1762/n2452/2326791.html.

101. On-line news. Retrieved on 16.Apr.2013 from http://www.soca.gov.uk/news/296-meter-cheater-fraud-rips-off-electricity-customers-.

102. On-line news. Retrieved on 16.Apr.2013 from http://www.soca.gov.uk/news/292-scareware-alert-to-web-users.

103. On-line news. Retrieved on 16.Apr.2013 from http://www.afp.gov.au/media-centre/news/afp/2010/november/media-release-operation-smashes-organised-crime-and-counterfeiting-syndicate.

104. On-line news. Retrieved on 16.Apr.2013 from http://www.afp.gov.au/media-centre/news/afp/2010/december/warning-on-new-internet-scams.

105. On-line news. Retrieved on 16.Apr.2013 from http://www.interpol.int/Crime-areas/Organized-crime/Asian-Organized-Crime.

106. On-line news. Retrieved on 10.Mar.2013 from http://www.fbi.gov/news/stories/2009/november/atm_111609.

107. On-line news. Retrieved on 10.Mar.2013 from http://www.fbi.gov/news/stories /2009/october/phishphry_100709.

108. On-line news. Retrieved on 10.Mar.2013 from http://www.fbi.gov/news/stories /2009/june/auctionfraud_063009.

109. On-line news. Retrieved on 10.Mar.2013 from http://www.mps.gov.cn/n16/n12 52/n1762/n2452/2260417.html.

110. On-line news. Retrieved on 10.Mar.2013 from http://www.mps.gov.cn/n16/n98 3040/n2040908/n2040938/2043555.html.

111. On-line news. Retrieved on 10.Mar.2013 from http://www.mps.gov.cn/n16/n98 3040/n2040908/n2040938/2043619.html.

112. On-line news. Retrieved on 10.Mar.2013 from http://www.mps.gov.cn/n16/n98 3040/n2040908/n2040938/2043573.html.

113. On-line news. Retrieved on 10.Mar.2013 from http://www.mps.gov.cn/n16/n98 3040/n2040908/n2040938/2043524.html.

114. On-line news. Retrieved on 10.Mar.2013 from http://www.mps.gov.cn/n16/n98 3040/n2040908/n2040938/2043611.html.

115. On-line news. Retrieved on 10.Mar.2013 from http://www.mps.gov.cn/n16/n983040/n2040908/n2040938/2043591.html.

116. On-line news. Retrieved on 10.Mar.2013 from http://www.mps.gov.cn/n16/n983040/n2040908/n2040938/2043581.html.

117. On-line news. Retrieved on 10.Mar.2013 from http://www.mps.gov.cn/n16/n1252/n1762/1798100.html.

118. On-line news. Retrieved on 10.Mar.2013 from http://news.sina.com.cn/w/2009-03-14/112315309043s.shtml.

119. On-line news. Retrieved on 10.Mar.2013 from http://news.xinhuanet.com/world/2009-02/25/content_10891681.htm.

120. On-line news. Retrieved on 10.Mar.2013 from http://www.afp.gov.au/media-centre/news/afp/2009/july/credit-card-manufacturing-equipment-seized-after-raids-on-6-million-syndicate.

121. On-line news. Retrieved on 09.Feb.2013 from http://www.fbi.gov/news/stories/2008/march/innocent_images030608.

122. On-line news. Retrieved on 09.Feb.2013 from http://www.fbi.gov/news/stories/2008/october/darkmarket_102008.

123. On-line news. Retrieved on 09.Feb.2013 from http://www.afp.gov.au/media-centre/news/afp/2008/May/sydney-man-linked-to-identity-theft-syndicate.

124. On-line news. Retrieved on 09.Feb.2013 from http://www.afp.gov.au/media-centre/news/afp/2008/December/22-identified-for-downloading-child-abuse-videos.

125. On-line news. Retrieved on 09.Feb.2013 from http://www.fbi.gov/news/stories/2007/june/gambling_060607.

126. On-line news. Retrieved on 09.Feb.2013 from http://www.fbi.gov/news/stories/2007/february/iptheft020107.

127. On-line news. Retrieved on 09.Feb.2013 from http://www.mps.gov.cn/n16/n1252/n1762/n2452/137073.html.

128. On-line news. Retrieved on 09.Feb.2013 from http://www.afp.gov.au/media-centre/news/afp/2007/February/ahtcc-warns-on-internet-employment-scams.

129. On-line news. Retrieved on 09.Feb.2013 from http://www.afp.gov.au/media-centre/news/afp/2007/June/afp-integral-in-international-hunt-for-on-line-predators.

130. On-line news. Retrieved on 09.Feb.2013 from http://www.afp.gov.au/media-centre/news/afp/2007/December/operation-irenic.

131. On-line news. Retrieved on 26.Jan.2013 from http://www.fbi.gov/news/stories/2006/june/iprny063006.

132. On-line news. Retrieved on 26.Jan.2013 from http://www.fbi.gov/news/stories/2006/march/cats030606.

133. On-line news. Retrieved on 26.Jan.2013 from http://www.fbi.gov/news/stories/2006/february/innocent_images022406.

134. On-line news. Retrieved on 26.Jan.2013 from http://www.mps.gov.cn/n16/n1252/n1762/n2452/128968.html.

135. On-line news. Retrieved on 26.Jan.2013 from http://www.fbi.gov/news/stories/2006/april/internet_trends040706.

136. On-line news. Retrieved on 26.Jan.2013 from http://www.fbi.gov/news/stories/2004/may/piracy_051704.

137. On-line news. Retrieved on 26.Jan.2013 from http://www.mps.gov.cn/n16/n1237/n1342/118206.html.

138. Qu Xuewu, on-line article, retrieved on 29.Apr.2014 from http://www.chinalawedu.com/news/16900/173/2004/9/re55364858341419400221750_132125.htm.

139. Österreiche Sicherheitsbericht 2013, retrieved on 15. June.2015 from http://www.bmi.gv.at/cms/bmi_service/start.aspx#t_download.

140. Österreiche Sicherheitsbericht 2012, retrieved on 15. June.2015 from http://www.bmi.gv.at/cms/bmi_service/start.aspx#t_download.

141. Österreiche Sicherheitsbericht 2011, retrieved on 15. June.2015 from http://www.bmi.gv.at/cms/bmi_service/start.aspx#t_download.

142. Österreiche Sicherheitsbericht 2010, retrieved on 15. June.2015 from http://www.bmi.gv.at/cms/bmi_service/start.aspx#t_download.

143. Österreiche Sicherheitsbericht 2009, retrieved on 15. June.2015 from http://www.parlament.gv.at/PAKT/VHG/XXIV/III/III_00186/index.shtml.

144. Österreiche Sicherheitsbericht 2008, retrieved on 15. June.2015 from http://www.parlament.gv.at/PAKT/VHG/XXIV/III/III_00099/index.shtml.

145. Österreiche Sicherheitsbericht 2007, retrieved on 15. June.2015 from http://www.parlament.gv.at/PAKT/VHG/XXIV/III/III_00034/index.shtml.

146. Österreiche Sicherheitsbericht 2006, retrieved on 15. June.2015 from http://www.parlament.gv.at/PAKT/VHG/XXIII/III/III_00114/index.shtml.

Appendices

Appendix 1: Abstract (Abstract of English Version and Keywords)

Organized crime is a common phenomenon and not strange for us, compared with it cyber crime can be said an emergent type of crime. The latter is usually closely linked with information communication technologies, which is tried to be utilized by all criminals worldwide. Beyond all doubt, the organized criminal groups also take full advantage of ICTs to commit organized crime worldwide. To some extent, the combination of transnational organized crime and cyber crime bring us a new type of crime, which is cyber transnational organized crime. In consideration of the increasing seriousness of cyber transnational organized crime, this dissertation focuses on its manifestations, the problems which have brought to criminal theories and judicial practices, and the proposals how to solve these problems. So this dissertation is divided into 6 chapters, respectively, Evolution of Organized Crime since 1950s and its concept, Characteristics and New Trends of Organized Crime in the Era of Internet, Investigations on Criminal Legislation and Adjustment of Criminal Policy Combating Cyber Transnational Organized Crime Worldwide in the Internet Age, The Dilemmas of Criminal Theory, Legislative Absence and Judiciary Obstacles when Combating Transnational Organized Crime Worldwide in the Era of Internet, Theoretical

Preparations and Legislative Countermeasures Combating Transnational Organized Crime in the Internet Era and Cooperation between Countries at the Regional and International Level Combating Transnational Organized Crime in the Internet Era.

Firstly, the chapter 1 demonstrates the development of organized crime and its concept. Because the history of organized crime provides us with a mirror for better understanding the organized crime under the internet age, some countries in Europe, North America, Asia and Oceanica are picked out as the representatives. In this chapter the concepts of some scholars and nations concerning organized crime are also introduced, by means of this introduction the core elements of organized crime's concept have been defined under the internet age.

Secondly, by means of analyzing 250 cases, the chapter 2 illustrates characteristics of present organized crime and new trends of organized crime, which will reveal the distinct characteristics of cyber transnational organized crime and its developing trend in the future, informatization of traditional transnational organized crime and transformation of cyber crime into organized cyber crime.

Thirdly, the chapter 3 focuses on investigations on criminal legislation and adjustment of criminal policy combating cyber transnational organized crime worldwide in the internet age. Like as the chapter 2, this chapter also takes some countries in Europe, North America, Asia and Oceanica to introduce their legislation and policy combating against organized crime and cyber crime. And this work can help us know the loopholes and weaknesses when fighting with cyber transnational organized crime.

Fourthly, the chapter 4 demonstrates dilemmas of theory of joint crime and resolutions under cyber transnational organized crime. Since cyber transnational organized crime usually involved in more than two countries, and it creates new challenges to the criminal theories and judicial obstacles. One obvious challenge is the dilemmas of the theory of joint crime. This chapter focuses on the evolution of the structure of traditional organized crimes, the theoretical problems brought by structure of cyber organized criminal groups and corresponding countermeasures.

Fifthly, the chapter 5 analyzes conflicts of jurisdiction and corresponding solutions of transnational organized crime in the internet era, these conflicts are other problems result in internet and internet-related ICTs. Under the circumstance of cyber transnational organized crime, the actus reus and criminal results are often located in different countries. As the matter of fact, more than two countries would claim criminal jurisdiction over this crime, and then the conflicts of jurisdiction will be increased more than before. After analyzing some theories and methods to solve criminal jurisdiction of cyber crimes, the principle substantive damage is advocated by this dissertation, which aims to reduce the increasing conflicts of criminal jurisdiction about cyber transnational organized crime.

Finally, the chapter 6 demonstrates solutions for informatization of traditional transnational organized crime and transformation of cyber crime into organized cyber crime. As the final chapter of this dissertation, it also can be said a summary of the whole dissertation. In order to effectively prevent cyber transnational organized crimes, two steps need to be done: firstly, this chapter reaffirms two trends of organized crimes, informatization of traditional transnational organized crime and transformation of cyber crime into organized cyber crime, which were proposed in chapter 2. In order to cope with challenges and dilemmas brought by these two trends, theoretical researches need

to be fully and deeply carried out by the theoretical communication; secondly, In view of cyber transnational organized crime cannot be definitely coped with by an individual country, regional and international judicial cooperation against cyber transnational organized crime is also urgent and important for the present situation, this chapter gives some proposals for combating against cyber transnational organized crimes.

This dissertation takes a perspective that how the transnational organized crime and cyber crime overlap and combine with each other, which brings us cyber transnational organized crime. The focuses of this dissertation deals with the dilemmas that are created by cyber transnational organized crime, finds the legislative loopholes in domestic law, regional and international conventions combating against transnational organized crime and cyber crime and gives some suggestive proposals to solve these problems. However, there is no end, the other new challenges are generated by cyber transnational organized crime still need to be further researched.

Keywords: Transnational Organized Crime, Cybercrime, Information Communication Technologies, Theory of Joint Crime, Jurisdiction, Informatization of Traditional Transnational Organized Crime, Transformation of Cybercrime into Organized Cybercrime

Appendix 2: Die Zusammenfassung(Abstract of German Version)

Organisierte Kriminalität ist seit Jahrhunderten ein bekanntes Phänomen. Verglichen hierzu ist die Internetkriminalität ein Phänomen, welche seit 20 Jahren besteht. Die Internetkriminalität ist verbunden mit Informationstechnologie, welche von Kriminellen

weltweit verwendet wird. Darüberhinaus hat die organisierte Kriminalität den Vorteil der Informations- und Kommunikationstechnologien, nämlich, ICTs, um weltweit organisiert diese auszuüben. Die Verbindung von transnational organisierter Kriminalität und Cyberkriminalität bingt einen neue Art von transnational organisierter Kriminalität hervor. Diese Dissertation behandelt basierend auf der immer mehr ernstzunehmenden transnational, organisierten Cyberkriminalität in 6 Kapiteln die Auswirkungen, zeigt neue Trends auf und beschreibt die juristische Praxis. Darüberhinaus werden Vorschläge zum Lösen dieser Probleme beschrieben.

Kapitel 1 beschreibt die Entwicklung der organisierten Kriminalität und deren Konzept. In diesem Kapitel werden Konzepte von Organisationen und Nationen gegen die organisierte Internetkriminalität und deren zentrale Elemente beschrieben.

Kapitel 2 behandelt 250 Fälle und charakterisiert die derzeit orangisierte Kriminalität, neue Trends und deckt auf den speziellen Charakter der transnationalen Cyberkriminalität und deren Entwicklung in der Zukunft.

Das 3. Kapitel behandelt die Nachforschung der bestehenden Legislative und der Regulierung sowie der Bekämpfung dieser transnationalen Cyberkrimialität. Diese Dissertation hilft die Gesetzeslücken und die Schwächen aufzuzeigen, welche in der Bekämpfung dieser Art von Kriminalität bestehen.

Das 4. Kapitel demonstriert das Dilemma dieser beiden Phänomen und Lösungen hierzu. Dieses Kapitel fokusiert sich auf die Entwicklung der Struktur der traditionell

organisierten Kriminalität und der theoretischen Probleme die durch die kriminellen Cyber – Gruppen entstanden sowie dazuführende Gegenmaßnahmen.

Kapitel 5 analysiert die Konflikte in der Legislative und der Lösung der transnational orgainiserten Kriminaltität in der Internetära. Es werden Theorien und Methoden beschrieben, um die Gerichtsbarkeit zu lösen. Das Ziel der Dissertation ist den Konflikt der traditionellen Kriminalität im Zusammenspiel mit der Cyberkriminalität zu reduzieren.

Kapitel 6 demonstriert Lösungen für die Informatisierung der traditionellen Transnational organisiertes Verbrechen und die Transformation der Cyber-Kriminalität in organisierte Cyberkriminalität. Letztes Kapitel ist eine Zusammenfassung der Disseration. Um effektiv eine transnationale Cyberkriminalität zu verhindern sind 2 Schritte notwendig. Erstens um mit den Anforderungen und den Zwiespalt der Cyberkriminalität effektiv entgegenzutreten muß die Kommunikation dieser verstanden werden. Zweitens regionale und international Rechtssprechung ist wichtig und muß angepaßt werden. Dieses Kapitel zeigt Vorschläge auf um das zu gewährleisten.

Diese Dissertation zeigt auf wie die transnational organisierte Kriminalität und die Cyberkriminalität überlappen und einander ergänzen und zu einer transnationalen organisierten Kriminalität werden. Es wird in dieser das Dilemma zwischen der regionalen Legislative und den internationalen Konventionen beschrieben und abschließend ein Lösungsweg aufgezeigt. Eine vollständig ganzheitliche Lösung kann nicht aufgezeigt werden und weitere Lösungen sind noch zu erarbeiten.

Appendix 3: Acknowledgement

As a doctoral candidate of University of Vienna in the major of criminal law, in 2011 under the supervision of Univ.-Prof. Dr. Susanne Reindl-Krauskopf and Professor.Yu Zhigang I started to carry out my research on Transnational Organized Crime in the context of Internet. I got my master degree in China University of Political Science in and Law in 2011, and in Zhengzhou Institute of Aeronautical Industry Management I got my bachelor degree. During my master academic study, I started to be interested in cybercrime and organized crime. At the end of 2011, fortunately, I got the chance that I can work with Univ.-Prof. Dr. Susanne Reindl-Krauskopf to continue my doctoral academic study and carry out my research subject. During the process of writing this dissertation, firstly, I want to express my appreciation to my supervisor Reindl-Krauskopf and my domestic supervisor professor Yu Zhigang, since they gave me a lot of useful suggestion about the structure. Especially professor Reindl-Krauskopf, as an excellent expert of computer law, environment criminal law and economic criminal law she introduced me to Mr.Mag.Maximilian Edelbacher. Of course Mr. Maximilian Edelbacher is another person I want to give my thankfulness. He is the expert of organized crime and final crime, the Hofrat of the Federal Police of Austria and served as the chief of the Major Crime Bureau, an international expert for the Council of Europe, OSCE and UNO. Thanks a lot for Mr. Maximilian Edelbacher give me advices about finding documents about organized crime. Finally, thanks for the help of Univ.-Prof. Dr.Walfgang Mazal, without his help I could not come to University of Vienna to continue my doctoral academic study. As the referees of my dissertation Prof Dr. Frank Höpfel and Prof. Dr. Christian Grafl gave me really pertinent remarks and suggestions for my dissertation, thanks a lot to Prof Dr. Frank Höpfel and Prof. Dr. Christian Grafl for their support. Finally, Graham Sedgley, as an English native speaker editor, he helped me correct the grammer mistakes. Anyway, it is very that with the help of professor Reindl-Krauskopf, professor Yu Zhigang, Mr.Mag.Maximilian Edelbacher

and professor Mazal, professor Höpfel, professor Grafl and Graham, i can finish my research subject and this dissertation. Thanks a lot for their contributions for my dissertation, here I express my heartfelt thankfulness. Their support and help are the motive force of my academic career, which support me to never give up in life.

Appendix 4: Curriculum Vitae

◆ Personal Data

Name： Li Xiangxia Gender：Female

Birthdate：1983-03-23 Martial：Single

Address: No. 35, Building 2, Unit 7, 103, Dayangyibin Lane, Dongcheng District,Beijing 100005,P.R.China.

Simmeringer Platz 1/1/27, 1110 Wien, Austria

Phone Number：+43-699-1720-1625

E-mail：lixiangxia29@gmail.com

◆ Brief Self-introduction

Since 2002 i started college study of Chinese law, and began to study criminal law since my master academic study in China University of Political Science and Law. At the end of 2011 I was supported by the China Scholarship Council to carry out my doctoral research subject in University of Vienna. During the past years, I worked as a lawyer's assistant for one year in China, and also as an assistant worked for the summer holiday program between China University of Political Science and Law and a Russian University, at the end of 2013 I was a volunteer of 2013 ACUNS Vienna Conference. Since I studied Chinese law for more than 10 years, especially Chinese criminal law, I have the abilities of dealing with the assistant job concerning law(especially at the Chinese law), being able to give lectures to college students and continuing my academic studies.

◆ Education

- Doctor Candidate 2011.12-2015.6 University of Vienna Criminal Law
- Master 2009.09-2011.07 China University of Political Science and Law Criminal Law
- Bachelor 2002.09-2006.07 Zhengzhou Institute of Aeronautical Industry Management Law

◆ Major and Research Area

Chinese Criminal Law, Comparative Criminal Law, Organized Crime, Cybercrime and so on.

◆ Scientific Achievements and Experience

1. The Relationship of Shadow Economy and Corruption in China, published in Maximilian Edelbacher, Bojan Dobovsek and Peter C.Kratcoski edc, *The Relationship of the Informal Economy to Corruption, Fraud and Organized Crime, 03.*2015 issued by CRC Press Taylor and Francis Group.
2. The Dissimilation of Joint Crime by Evolution of Structure of Organized Criminal Groups in Cyberspace, Wang Jian edc, *Foreign Experiences of Internet Law and the Choices of China*, November of 2014,China Legal Publishing House.
3. The Empirical Analysis and Counter-measure of Chinese Citizens' Transnational Crime Under the Background of Information Age——Base on 340 Cases between 2003 to 2012, Journal of National Prosecutors College, 2014,Issue 1.
4. Participating the project of translating international laws in 2014, and translated REGULATION (EC) No 1211/2009 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 25 November 2009.
5. Participating in the significant Ministerial Project of China Law Society of 2011: Systematic Research on the Legislation of Cybercrime, Serial number: CLS（2011）B25.
6. Participating in the significant project of Supreme People's Court in 2011: "Research on the Punishment and Prevention of Slander and other crimes via Internet".
7. Participating in the significant social science project of the Ministry of Education in 2012: "Research on the Overall Construction of Internet Legislation in the Information Era", Serial number: 12JZD039.
8. Participating in National Nomocracy and Juristal Theory Research Project of Ministry of Justice: "Research on New Transnational Crime under the Information Environment of Globalization".
9. From December of 2011.12 to July of 2014, under the supervison of Univ.-Prof. Dr. Susanne Reindl-Krauskopf carrying out the project of Transnational Organized Crime under the Background of Internet within the scope of Europe, after the data collection and analysis, at present this project is under the researching phase, the part that in my charge and the final result will be my doctoral dissertation of University of Vienna.

◆ Academic Training and Activities

1. From March of 2012 to June of 2012, participated in the seminar of methodology of jurisprudence which organized by Univ.-Prof. Dr. Christian Stadler.
2. From March of 2012 to June of 2012, participated in the course of Austrian Legal System which lectured by Mag. Verena Haas.
3. Between 07.10.2012 and 10.10.2012, jointly sponsored by University of Vienna and China University of Political Science and Law: SOCIAL SECURITY IN TIMES OF ECONOMIC TURBULENCES.
4. On 17.10.2012, Academic Council on the United Nations System sponsored (Vienna)——6th session of Conference of the Parties to the United Nations Convention against Transnational Organized Crime, side event to introduce TIPP (Trafficking in Persons Platform) of the International Association of Prosecutors (IAP).

5. From October of 2012 to December of 2012, participated in the Seminar of Judicature and text analysis which organized by Univ.-Prof. Dr. Peter Fisher.
6. From October of 2012 to December of 2012, participated in the Course of the United Nation and Crime Prevention which lectured by Univ.-Prof. Dr. Slawomir Redo.
7. On 07.11.2012, the financial crime report of Mr. Maximilian Edelbacher：Financial Crimes——A Threat to Global Security.
8. From October of 2012 to December of 2012, participated in the Course of Professional Legal Writing in English which lectured by Christian Jensen.
9. From October of 2012 to December of 2012, participated in the Seminar of Criminal Law and Criminal Procedure Law which organized by Univ.-Prof. Dr. Frank Höpfel and Univ.-Prof. Dr. Manfred Hochmeister.
10. On 26.11.2012, Academic Council on the United Nations System sponsored (Vienna): Symposium on Femicide.
11. From October of 2012 to December of 2012, participated in the Seminar of Criminal Law and Criminology which organized by Univ.-Prof. Dr. Helmut Fuchs.
12. On 11.12.2012, jointly sponsored by United Nations Office on Drugs and Crime (UNODC), United Nations Information Service (UNIS)，International Organization for Migration (IOM),The University of Vienna, United Nations Academic Impact in Action, Academic Council on the United Nations System (ACUNS) and the other universities and educational training institutions worldwide: the webinar "Trafficking Prevention and Victims: New United Nations and Academic Perspectives".
13. Between 08.01.2013 and 11.01.2013, Academic Council on the United Nations System sponsored (annual conferences in Vienna): HAVE THE UNITED NATIONS AGENCIES ADAPTED TO THE 21th CENTURY?
14. From March of 2013 to June of 2013, participated in the seminar of the United Nation and Criminal Law which organized by Univ.-Prof. Dr. Frank Höpfel and Univ.-Prof. Dr. Slawomir Redo.
15. ON 13.05.2014, ACUNS Vienna Liaison Office and the Government of Austria: Elderly as Victims of Corruption。
16. ON 14.05.2014, ACUNS Vienna Liaison Office and the Government of Austria: Relationship of Organized Crime and Informal Economy.