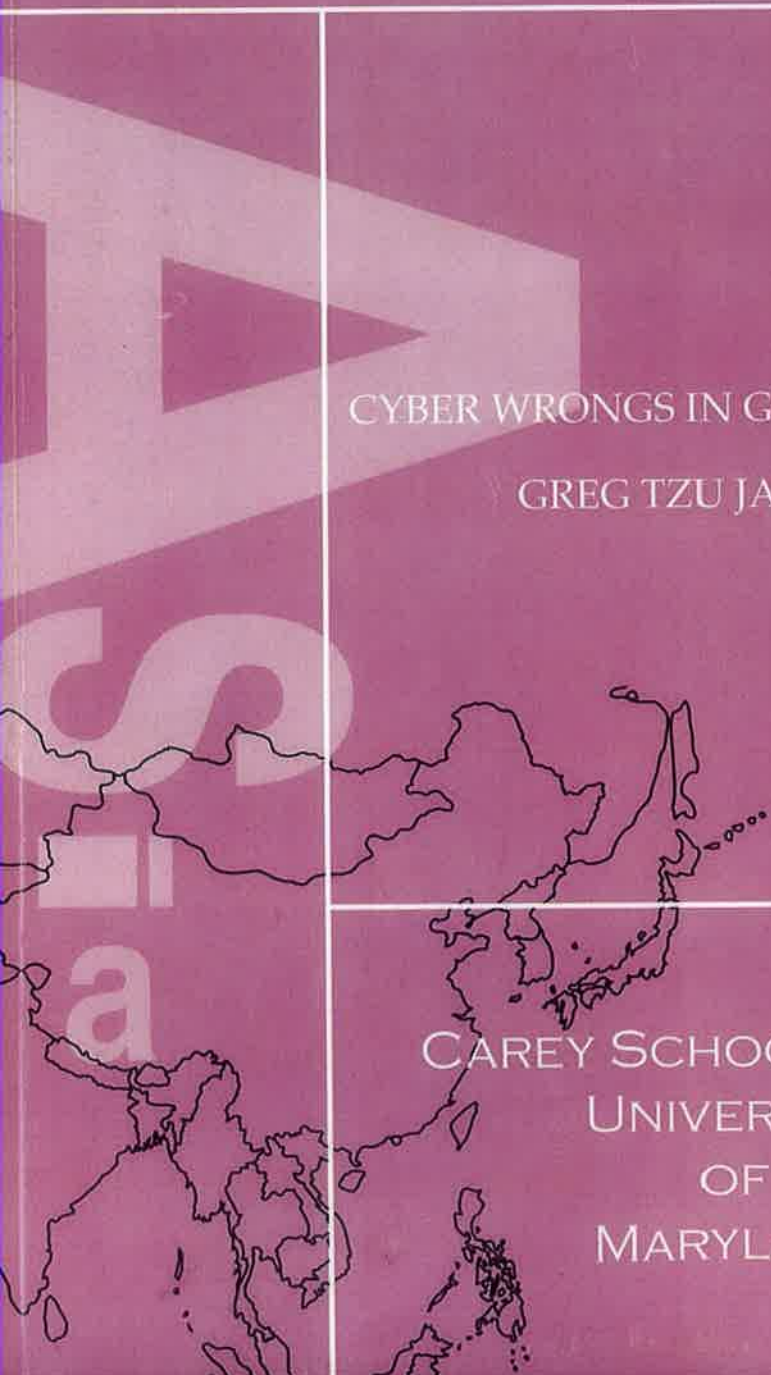


Maryland Series in Contemporary Asian Studies

Number 4 - 2016 (227)

CYBER WRONGS IN GREATER CHINA

GREG TZU JAN YANG



CAREY SCHOOL OF LAW
UNIVERSITY
OF
MARYLAND

Maryland Series in Contemporary Asian Studies

General Editor: Michael Van Alstine

Executive Editor: Chih-Yu T. WU

Associate Editor: Matthew Lyon

Managing Editor: Chih-Yu T. WU

Assistant Editor: Rebecca Shin

Editorial Advisory Board

Professor Robert Sutter, George Washington University

Professor Bih-jaw LIN, National Chengchi University

Dr. Ying-jeou MA, Chinese Society of International Law

Professor Zhaojie LI, Tsinghua University

All contributions (in English only) and communications should be sent to:

Chih-Yu T. WU

University of Maryland School of Law

500 West Baltimore Street

Baltimore, Maryland 21201-1786, USA

All publications in this series reflect only the views of the authors.

While the editor accepts responsibility for the selection of materials to be published, the individual author is responsible for statements of facts and expressions of opinion contained therein.

Subscription is US \$50.00 per year for 4 issues (regardless of the price of individual issues) in the United States and \$60.00 for Canada or overseas. Checks should be addressed to MSCAS.

Tel.: (410) 706-3870

Fax: (410) 706-1516

Price for single copy of this issue: US \$18.00

ISSN 0730-0107

ISBN 1-932330-57-7

© Maryland Series in Contemporary Asian Studies, Inc.

CYBER WRONGS IN GREATER CHINA

Greg Tzu Jan Yang*

TABLE OF CONTENTS

I.	CYBER WRONGS IN GENERAL	2
II.	CYBER FRAUD.....	4
	A. The Characteristics of Cyber Fraud.....	4
	B. Phishing (Web Phishing)	5
	1. <i>Case Study - Web Phishing</i>	5
	C. Web Shopping Fraud	6
	D. Misrepresentation of Goods in Web Shopping.....	8
	1. <i>Case Study - Wrong Teddy Dog</i>	8
	E. Investment Scam.....	9
III.	CYBER THEFT	10
	1. <i>Case Study - QQ Account and QQ Coin Thieves</i>	14
	2. <i>Case Study - Cyber Game Equipment Thief</i>	16
IV.	HACKER	17
	1. <i>Case Study - Underage Hacker</i>	19
V.	DEFAMATION	20
	1. <i>Case Study - The SONE Zue De Defamation Case</i>	23
	2. <i>Case Study - Defaming the Government</i>	24
VI.	CYBER HYPER	25
	A. Traditional Order and Value	27
VII.	CYBER HITMAN	28
	1. <i>Case Study - The Yili QQ Star Milk</i>	28
VIII.	CYBER PORNOGRAPHY	29
	1. <i>Case Study - Watching Pornography in Private Dwelling</i>	32
	2. <i>Case Study - LI Zhong Rei Drug and Rape Case</i>	33
	A. Naked Chatting and Cyber Sex.....	35
IX.	THE TAIWANESE FIRST COMMERCIAL BANK HEIST	35
	A. Background.....	36
	B. Where Did the Money Go?.....	37

* Greg Tzu Jan Yang, SJD, Bond University, Australia. PhD Peking University, China. Assistant Professor, China University of Political Science and Law, College of Comparative Law.

C.	The Suspects Arrested	38
D.	Ministry of Justice Investigation Bureau, Cyber Forensics Laboratory	40
E.	The ATM Machines Itself	41
X.	AN INTERVIEW WITH AN INSIDER.....	43
A.	Recommendation from the First Commercial Bank Heist....	44
XI.	CONCLUSION	45

I. CYBER WRONGS IN GENERAL

Greater China refers to Mainland China (China), Hong Kong, Macau and Taiwan. Mainland China is the People's Republic of China (PRC). Hong Kong and Macau is its "special administrative region" (SAR). Taiwan is officially known as the Republic of China (ROC). Though there are some political issues between Mainland China and Taiwan, the problem facing Mainland China is also faced by Taiwan and *vice versa* since cyber wrongs are borderless. Thus, this article will discuss cyber wrongs in Mainland China, in addition to an important and recent case, which occurred in Taiwan.

Cyber wrongs cover cybercrime and cyber torts. Traditionally speaking, when we talk about tortious liability and criminal liability, although there are a lot of similarities between the two, they are still two different sets of laws. One major difference is the standard of proof. In criminal law, guilt must be proven beyond reasonable doubt. Under the law of torts, if one satisfies the balance of probability, it would be sufficient to find one liable.

Another difference is that in the common law society, criminal liabilities involve police. When we talk about torts, usually it would be seen as a civil matter and normally the police would not be involved. This is not necessary the case in China when we talk about cyber wrongs.

China has one of the largest internet users in the world. Up until 2013, there were 590,560,000 people hooked to the internet.¹ Attached to this enormous number of users is, of course, a huge amount of infringement cases. Currently, based on many cases and practical experiences, many of these cases had a tortious nature but, nevertheless, were channeled through criminal proceedings with police involvement.

1. Sina Technology News "China has 5.91 hundred million net users and 4.64 hundred million mobile phone users," <http://tech.sina.com.cn/it/2013-07-17/14088548488.shtml> 2013-07-17.

This may reflect the reality of China's current legal practice, as police do not get involved with pure civil cases. Since evidence discovery in China is a major problem in any kind of civil case, in which China does not have the system of interim injunctions for evidence discovery, there are many difficulties of discovery when dealing with the internet and computer. Thus, in China, when one tries to seek the remedy for infringement of their legal right in cyber spaces, without a criminal channel and police involvement, their chance of achieving the desired remedies would be very slim. One exception to this is defamation, in which one could seek pure tortious damage.

Therefore, as tortious remedies are more abstract than criminal sanctions in China, when we talk about cyber wrongs, people usually point to criminal sanctions, such as cyber fraud, theft, hackers and cyber pornography i.e. cybercrime. In this chapter, cybercrimes and cyber wrongs will be equally used in many regards, if not specifically talking about cyber torts.

With a more tortious side of cyber wrongs, defamation would be looked into. However, defamation in China also mostly lean towards criminal sanctions. Another type of cyber wrongs, perhaps more unique in China, is known as "cyber hyper" and "cyber hitman." Cyber hitman is theoretically illegal in China but is difficult to identify and prosecute. On the other hand, the legal position of cyber hypers are unclear. Currently there are no laws that clearly suggest this kind of practice as legal or illegal. However, on August 2013, the Chinese government arrested two famous cyber hypers known as "Li Er Chai Si" (立二拆四) and "QIN Huo Huo" (秦火火) for spreading rumors and defaming a public figure.² This is interesting because this shows that the Chinese government is willing to battle this kind of practice head on and that a more related law may be implemented accordingly.

Besides a more general or traditional kind of computer wrongs, the central concept has not been much more than physical crimes, even though it is quite low tech. Instead of saying it is a cybercrime, it is, in many regards, a mind game. For example, in cyber phishing, it is really a battle between the fishermen (cybercriminal) and the fish (the victim). However, on July 10, 2016, when a bank in Taiwan was heisted by foreign criminals by malwares implemented into that bank's internal system, the bank's

2. Baidu Encyclopedia "Li ER Chai Si" http://baike.baidu.com/link?url=H04qL_UWRsXhuwrjo9az6F67612kBE8e8dqeEMIVYT06LiIFEm5VvUTqcGIdhiGR21SwF6kFUvYyYB7GiV4L6tNGF3zxXe_M0rzrvUkNW3cO.

ATM machines were spilling cash, though no one was physically controlling it. This is perhaps a new kind of computer theft, with a large amount of commercial consequence.

II. CYBER FRAUD

According to the People's Republic of China Criminal Code (中华人民共和国刑法) Article 287:

Whoever uses a computer for financial fraud, theft, corruption, misappropriation of public funds, stealing state secrets, or other crimes is to be convicted and punished according to relevant regulations of this law.

Therefore, when we talk about cyber fraud, this could be seen as divided into two categories: fraud which involves cyber technologies, such as phishing (web phishing), and using the web as a medium to perform traditional fraud, such as shopping fraud, misrepresentation of goods, false advertisements, etc.

A. The Characteristics of Cyber Fraud

Fraud means one cheats another person into believing in something that either does not exist or into believing something that is inconsistent for economic gain or other. The important element is intent (*mens rea*): whether the original cheater had the intent of creating such fraud. If, however, fraud was only the consequence and the original creator did not possess the relevant intent for making such a fraud, then the matter may be misrepresentation instead of fraud.

Cyber fraud indicates offenses that are being carried out by the criminals with the computer network and internet facilities. Originally, computer frauds were limited to the extent of stealing data, tampering records and account balances, stealing bank accounts and salary payments, etc. However, with the world-wide connection of the internet, the possibilities of committing fraud have increased beyond national borders. Now it usually involves a scheme that aims to make people believing a particular scenario so they can cheat them into spending money or transferring funds.

Certain inherent features of internet, such as anonymity, cost effectiveness, breadth of reach, difficulties in authenticating identity, etc. have made it difficult to check fraudulent acts. A fraudulent investment scheme that looks credible and genuine may be advertised all around the world within seconds by internet and through email service. Computer fraud is much easier since they can find gullible customers in large number through the internet service. The possibility of such fraud is obvious in the field of

e-commerce, where goods and services are obtained online and payments are made through credit cards or other instruments.

B. Phishing (Web Phishing)

As mentioned previously, cyber fraud usually involves creating a scheme that aims to cheat people into believing a particular scenario to spend money on. Thus, phishing is the most obvious. Phishing means web fishing, a combination of the word phone and fishing. It usually entails a person sending out fraudulent emails or creating a website people believe is from a credible source and is willing to submit their credit card password, identification card numbers, computer account passwords, etc. Phishing uses the information in furtherance of a crime, such as stealing credit card funds, using people's identity to do other illegal activities, or creating another bigger fraud based on the information they fished.³

It used to be that stealing people's internet online time was one of the major characteristics for this kind of fraud, especially when a person could only get access to the internet for a certain period of time and had to pay internet service providers for more time. Phishing allowed a person to access another person's internet account and use up that person's time allowance without paying. However, with the advancement of technology, most of the internet providers, at least in China, allow their subscribers to access the internet without time or data limitations for a set amount of fee. As a result, this kind of fraud basically has disappeared in China. On the other hand, in countries like Australia where internet accounts are based on data usage due to bandwidth limitation, this kind of fraud still applies to this type of account users.

1. Case Study - Web Phishing

One day, Professor X's friends suddenly received an email from him saying Professor X has been arrested in some Eastern European country, urgently needs some money to settle the matter, and to transfer certain amounts of money to a particular account. Some of his closer friends, after receiving the email, were worried and transferred the set amount of money into that account. A few days later, they met with Professor X and to their surprise Professor X never left Beijing. Professor X did not know anything about the matter at all. After their investigation, Professor X finally remembered that he has an email account in "yahoo.com.cn." There was an email sent to him from the so called "yahoo administration," informing

3. Ji Jing and Zhang Zhi Chao "A Study on the New Type of Cyber Criminal Behavior" Chinese Public Prosecution Bureau Publishing Co., 2012 page 30.

him for the purpose of maintenance of his email account, his account name and password were needed. Following the administration's instruction, Professor X submitted it. As Professor X does not use his email account very frequently, he never noticed his email account passwords have been changed and emails were sent out to his contacts from his account on time. As a result, he could not access his email anymore as it has been hijacked from someone else by changing his passwords. His friends who wired money to that account all become the victims of fraud. Of course they reported the matter to the police immediately but as the account they wired money to was an overseas account, the Beijing police was limited in things they could do.⁴

C. Web Shopping Fraud

Web shopping fraud occurs when a seller is depicted as an online merchant, sells a particular product with the condition of payment first then delivery of goods, the good never arrives to the buyer, and the seller disappears from cyber space.

Although this is a classic case of cybercrime, the scam itself is nothing new. During the age of newspapers, this kind of fraud happened occasionally. Under the computer age, the internet and online shopping websites made it easier for criminals to perform this kind of fraud online.

With the situation in China, web shopping fraud could be divided into three categories, fraud done from an online shopping website, such as Taobao (淘宝), by creating a website by himself, and creating a website that imitates an established, well-reputable shopping website.

With the first kind of shopping fraud, you rarely see them occur on most reputable online shopping websites, such as Taobao or Alibaba (阿里巴巴), because they all have an internal checks and balance insurance policy and are done by payments to the third party, such as "Zhi Fu Bao" (Payment Treasure) (支付宝). However, during the earlier days when China was still developing online shopping companies, fraud was indeed a major concern. This kind of fraud, however, does not only occur in China. The author had an experience in Australia in 2003 when the author won an auction from EBay in the United States. After I paid the auctioneer by credit card, the goods were never sent to Australia and the auctioneer became uncontactable. Due to the fact that the amount of money involved in this matter was not much, I did not take any further action. It was only after a few weeks when the police from a county in the United States contacted me about the matter and informed me that many other victims were

4. Based on a true case.

involved in this scam, as well. He asked me if I could provide any information about the auction to assist in their investigation. I did and that was the last time I heard anything about the matter. Again, that happened almost 10 years ago. Although this kind of fraud does not happen as often, it still occurs from time to time.

The other form of online shopping fraud is when the criminal creates a website and uses that website to defraud people. This actually has not changed much from when people used newspapers to create fraudulent advertisements. The only problem is, due to the wide coverage of the internet, the power of such a scam could be widespread and affect many potential victims. Another serious problem for this kind of website is that it is easy to create, easy to put in many fraudulent certificates to persuade people into believing the credibility of the website, and it is with relative low cost. In addition, it would be difficult for law enforcement to enforce against since these kinds of websites suddenly appear and disappear. For example, in 2007 Mr. Hu purchased a Sony laptop from a website based in Shanghai. After payment, he received the parcel. Instead of a Sony laptop, the box was full of washing powders. The website disappeared and the seller became unaccountable.⁵ Currently, although the law enforcement agencies in China endeavor to battle against this kind of website and practice, the reality is these cases still occur every year. It is indeed almost fair to say that in China, if you want to buy something from the internet, unless you are dealing with a larger and more reputable online shopping web, it would be *caveat emptor*!

The third type is creating a website that looks like a known reputable shopping website but actually is not. In another words, passing off or fake website for the purpose of fraud. Website passing off used to be a very serious problem in China. For example, a website may be deliberately created making people believing it to be the Apple Company online shop, but in fact it's not. Once if you deal with this kind of so called "authentic online shop" then your interest is at the mercy of the criminals. It used to be a very serious problem in China, in fact not only the passing off of web shops but also actual shops. There has been cases of shops fraudulently passing off or even pretending to be the official shops for famous product brands.⁶ However, after the effort by the Chinese government, now it is rarer to see a website deliberately pretend to be another reputable or famous web shop. However, for the less famous or less well-known web

5. Ji Jing and Zhang Zhi Chao "A Study on the New Type of Cyber Criminal Behavior" Chinese Public Prosecution Bureau Publishing Co., 2012 page 47.

6. Soho Technology News "Chinese fake Apple Shop has been busted by foreign media, their fake products can almost compete with the real one." <http://it.sohu.com/20141225/n407272684.shtml> 2014-12-25.

shop, the problem of passing off is still widespread in the Chinese cyber space.

Generally speaking, web shopping fraud is a kind of fraud that is so wide that the exact type of web shopping fraud is only limited by imagination. In fact, the seller could also be defrauded by the buyer as well. For example, a buyer makes a purchase with the seller to first to gain his trust and then orders a large quantity of goods from the seller and asks the seller to send the goods first and then the buyer pays later. Usually for this type of arrangement, the seller would refuse it but due to the large amount and profit, and that the two parties had done deals before, the seller may agree to the arrangement. Once the goods have been sent to the buyer, the buyer would never pay and would have disappeared.

D. Misrepresentation of Goods in Web Shopping

Misrepresentation of goods occurs in a contract when the offeror and offeree thought they were dealing with the same subject matter but in fact were not. For example, the offeror offered to sell a plastic human skull but the offeree purchased the skull thinking it was an authentic human skull.

The difference between misrepresentation and fraud is that misrepresentation does not require an explicit intent to cheat (*mens rea*). In practice, this may not be easy to prove whether a particular online seller had the intent of deliberately misrepresenting the thing. When dealing with misrepresentation, on a pure legal analysis, that is without any ill intent, this may just be a contract law matter, e.g. without the meeting of mind. Thus, the contract entered between the seller and buyer may be void. It is possible to ask the seller to refund any money used to purchase the misrepresented goods. If, however, misrepresentation was done deliberately, then this would be a kind of fraud.

1. Case Study - Wrong Teddy Dog

In 2011, Ms. Lu from Qingdao, Shandong Province (山东省青岛市) saw someone advertising an offer to sell "Teddy Dog" (Toy Poodle) for RMB\$1800, in which the market price for such kind of dog would cost around 4000 – 5000 RMB. After few rounds of bargaining, Ms. Lu managed to bring down the price for the dog to RMB\$800, agreed upon by both parties. Originally, Ms. Lu thought she got a bargain but after the dog was shipped to her, she shockingly discovered that the dog was not a "Teddy Dog" but just a normal dog that was worth no more than a few

hundred RMB.⁷ Ms. Lu contacted the seller but the seller admitted no wrongdoing and refused to refund.

With the case above, the seller never disappeared but just refused to admit any wrongdoing. Due to the low loss suffered from Ms. Lu, Ms. Lu never bothered to take this matter into the court. However, if we analyze this case by pure legal means, then we can see there was obviously a misunderstanding between the seller and Ms. Lu. The question is whether during the process of their bargain, the seller realized the occurrence of a misunderstanding amounted to a misrepresentation. If the answer is positive, then this would be the seller doing something deliberate, and thus would be fraud. If not, it would depend on the evidence, such as corresponding emails between both parties, to determine whether an innocent misrepresentation may or may not have occurred.

E. Investment Scam

Investment scam is under the arena of white collar crime. Cyber investment scam is no different from a traditional investment scam. Just like other areas of cyber fraud, once the internet becomes the medium for such a scam, the width of the coverage for such scam suddenly becomes worldwide. Cyber investment scam usually involves sending out emails or spreading news about a particular scheme that once invested, the return would be exceptionally high. In China, a lot of investment scam websites are websites of shared investments, lotto number predictions, company or business investments, etc. Some of these websites are a passing off, made to imitate legitimate investment houses. Others are websites or email senders promoting certain investments, usually with an unreasonably high investment return. A unique type of scheme in China is the so called "Lotto Number Prediction" website, which is worth a closer look.

China bans gambling, except the so-called "Sports Lotto" (体育彩票) is allowed in China. It is called a sports lotto because the purpose is to raise capital to support sports development and is run by the sporting agency. There is no difference between this and other types of lotto in which every month winning numbers are drawn from different ping pong balls. In other words, this is a game of pure chance. The only problem is that Chinese people do not believe in the credibility of the lotto agency. They believe that there is insider information in regards to the ultimate winning numbers. Therefore, under this mindset, websites claiming to be able to "predict" the winning numbers (e.g. having connections with high officials) started to spur in the cyber world. To get their prediction services

7. Ji Jing and Zhang Zhi Chao "A Study on the New Type of Cyber Criminal Behavior" Chinese Public Prosecution Bureau Publishing Co., 2012 page 47.

from these websites, people had to purchase their membership first, with the cost of each level of membership being different and VIP membership costing the most. The prediction services do not just sell the insider winning numbers to their members, since that would be illegal. Instead, they predict different sets the most probable winning numbers, letting all members "invest money" to purchase a large quantity of different sets of numbers. If a prize won, then they will divide the "dividends" to each member depending on how much you invest.⁸

As you can see, the prediction of sports lotto numbers gathers members to invest on the purchase of lotto tickets, which may not be illegal. After all, the larger the purchase of numbers, the bigger the chance of winning. The problem, however, exists when those websites claim to use the investment funds from their members to purchasing lotto tickets when in fact they do not. They may use the money for their own use or pleasure, which may constitute an act of theft.

III. CYBER THEFT

First of all, let us look at the general definition of theft in China. According to the People's Republic of China Criminal Code, Article 264 provides us with a general definition of theft. Article 264 stipulates:

Those who steal relatively large amounts of public or private property and money or have committed several thefts are to be sentenced to three years or fewer in prison or put under criminal detention or surveillance, in addition to fines; or are to be fined. Those stealing large amounts of property and money or involving in other serious cases are to be sentenced to three to 10 years in prison, in addition to fines. Those stealing extraordinarily large amounts of property and money or involving in especially serious cases are to be sentenced to 10 years or more in prison or given life sentences, in addition to fines or confiscation of property. Those falling in one or more of the following cases are to be given life sentence or sentenced to death, in addition to confiscation of property:

- (1) Those stealing extraordinarily large amounts of money and property from financial institutions;
- (2) those committing serious thefts of precious cultural relics.

According to the above section, the main emphasis is money and property or any public or private property with value. This article, when

8. Sina Technology News "The Police are cracking down on illegal lotto prediction websites," <http://sports.sina.com.cn/1/2013-08-22/09316736267.shtml> 2013-08-22.

dealing with normal conventional property, is relatively straight forward. Although there was a constitutional issue with the recognition of "private property," that dispute has been settled recently.⁹ Accordingly, the obvious issue now is whether cyber property could be seen as property with value in the conventional sense.

In order to determine this, the PRC Criminal Code also provided regulations in regards to this. According to Article 287:

Whoever uses a computer for financial fraud, theft, corruption, misappropriation of public funds, stealing state secrets, or other crimes is to be convicted and punished according to relevant regulations of this law.

Based on Article 287, the PRC Criminal Code recognizes the use of a computer as a means of achieving the crime of theft but not a single category as a kind of crime itself. In other words, Article 287 recognizes the use of computer as a means of committing a crime. However, the main body of such criminal behavior is still determined by Article 264. Based on this, when we look into cyber theft, the main question that must be asked is, what kind of property has been stolen and whether that property could be determined as property with value in the normal legal sense.

Before determining whether one commits the crime of fraud, two requirements must be satisfied: the age requirement based on the Chinese Criminal Code and *mens rea*, the guilty mind or, based on the Chinese definition, "the subjective intention" of the perpetrator. The age requirement is 16 years of a natural person.¹⁰ The subjective intention requirement, however, is a little bit interesting. The requirement is very much similar to the *mens rea* requirement of common law jurisdiction. You must have a guilty mind when committing the crime.¹¹ If one objectively satisfies a possible criminal behavior without the subjective intent, although that person may not totally avoid criminal liability, that person certainly would have a very good defense from prosecution. The situation in China may not be as complicated as the common law requirements but, nevertheless, the subjective intent of the person being prosecuted still needs to be proven. The subjective intent requirement may not be complicated in a real world theft but under a cyber-scenario the problem of subjective intention may not be easy to determine. For example, under the example of Peer to Peer (P2P) downloading, we all know that under the Chinese law,

9. Sina News "Peking University Professor claims the new property law unconstitutional in an open letter, the debate between capitalism or socialism raised again." <http://news.sina.com.cn/c/2006-02-23/15019183436.shtml> 2006-02-23.

10. The People's Republic of China Criminal Code Article 17.

11. *Ibid.*, Article 14.

uploading questionable materials, such as pornography or copyrighted movies, onto the internet is illegal.¹² Downloading such materials for personal use is usually not seen as an illegal behavior, although the law in the area of downloading materials is not totally clear yet. One of the functions of the P2P downloading, such as Bit download, is that while you are downloading a particular material, you are at the same time also uploading it to the web for others to share. Thus, if you are downloading something, you may not know you are uploading at the same time—without “subjective intention.” So far this situation does not have any precedents at hand. However, these types of cases happened in Taiwan, which will be discussed later when we deal with internet pornography.

Now, let's get back to the discussion of “property” in the computer crime context, mainly pointing to “Personal Property.” According to The General Principles of the Civil Law of the People's Republic of China (《中华人民共和国民法通则》), Article 75:

A citizen's personal property shall include his lawfully earned income, housing, saving, articles for daily use, art objects, books, reference materials, trees, livestock, as well as means of production the law permits a citizen to possess and other lawful property.

A citizen's lawful property shall be protected by law, and no organization or individual may appropriate, encroach upon, destroy or illegally seal up, distrain, freeze or confiscate it.

Personal property in China, although it does not have any finer definitions besides the Civil Code, could be interpreted as any type of personal belonging that possesses certain monetary value that is capable under the law to be protected. Accordingly, this definition is fine with the traditional sense of theft but this may or may not be easily applicable under the scenario of cyber theft. Could the materials being stolen via means of computer be able to be determined as a property that is able to be stolen? This is due to the reasons in three areas:

1. The materials that cyber theft steals could be intangible information, such as credit card numbers, passwords or transfer of funds, etc.
2. With respect to so called tangible materials stolen via computer means, we are mostly talking about cyber money, cyber service (e.g. password for software updating), and equipment used in cyber games

12. The Interpretation of the Supreme People's Court and the Supreme People's Procuratorate on Several Issues concerning the Concrete Application of Law in the Handling of Criminal Cases of Making, Reproducing, Publishing, Selling and Spreading Pornographic Electronic Information by Means of the Internet, Terminal of Mobile Communications and Sound Message Stations, 2004.

that could be traded with real money in the real world. These materials, when compared with materials that has been stolen in the conventional world, is still relatively “intangible.”

3. Regardless of point one or point two, how do you value those cyber properties? As we know from the Civil Code of China, you must be able to have a value first in respect to the property in question, before the things are capable of being stolen.

With the logic derived from the three points above, the next question would be, how does one value cyber property, which is mostly intangible? As a result, when we talk about the value of cyber property, the value type could be again further divided into four kinds:

- First type - The property itself has value. For example, stolen money and transferred funds from a bank account via computer means.
- Second type - The thing that has been stolen is the key that leads into gaining or retrieving assets that are valuable. For example, the password of cyber bank account or any kind of password that leads to good or services that are capable of being physically stolen in the real world.
- Third type - Passwords that lead to certain communications account such as QQ, Weibo, or WeChat, (Facebook are not connectable in China currently), in which it itself does not have any set value but may leads to things or information that may contain monetary value
- Fourth type - This is the kind of property that is most disputed. It consists of equipment within the computer games that are tradable in the real world with real money. The main dispute for this kind of property is whether this type of asset can be seen as real “property,” protected under the relevant Chinese law and how to value them.

The first two types of cyber property have usually been regulated by Article 287 of the Criminal Code and possibly Article 286, which deals with hacking and cracking, as well. This is because the amount of theft valued is usually easier to determine with these two types of cyber theft. However, when looking at the third and fourth type of cyber theft, it may not be so easy to prosecute, as the value of the damage suffered by the victim is not easy to determine. Not to mention, with type four of the theft, it is yet to be determined whether the things stolen could be seen as property.

Let us look closely at type three of the cyber theft, which doesn't exist only in China. It is not uncommon to hear that people's passwords for Facebook, twitter, or QQ were stolen from the web. In fact, some of us may personally experience this type of computer crime, as well. A crime that no doubt occurs in most of the jurisdictions around the world. However, the person who experienced such instances may choose not to make a fuss,

as it may involve lengthy investigations that usually leads to no conclusion. However, what if the name of the account stolen has a high monetary value? For example, the most widely used cyber communication tool in China is the service know as QQ. The QQ service is similar to MSN (now ceased to exist) or ICQ (which still exists but with little use). Although superstitions, lucky numbers are a Chinese tradition, especially the number 8 and 6, in which 8 means rich and prosperity and 6 means lucky in Chinese.¹³ There was a funny incident back in June 6, 2006, in which the date contained 666. During that day, a lot of western pregnant ladies asked their doctors to help them avoid giving birth to their child on that day since 666 represents the devil in Christian religion. On the other hand, a lot of Chinese pregnant ladies rushed to the hospital, on that same day, in hopes to birth their babies on the 666 day.

In Hong Kong, due to this mentality, people are willing to spend a lot of money on license plates that contain good numbers such as 8 or 6. Thus, the Hong Kong government reserved the "lucky number plates" for auction. The same kind of mentality occurred in the Chinese cyber world, especially for business people using their cyber accounts for business communications. Though it is not easy for someone to steal others people's license plate, (and even if it were stolen, the usefulness of the plate is small), it is quite easy to steal other people's cyber account such as QQ. This can either be done by hacking or phishing but currently there is not much of a law in China to sanction this kind of behavior besides Article 252 of the Criminal Code. Article 252 of the Criminal code provides:

Those infringing upon the citizens right of communication freedom by hiding, destroying, or illegally opening others' letters, if the case is serious, are to be sentenced to one year or less in prison or put under criminal detention.

In other words, this article mainly deals with the freedom of communication instead of computer related matters.

1. Case Study - QQ Account and QQ Coin Thieves

In 2005, Mr. King¹⁴ established three workshops in Liaoning province (辽宁省) and employed 11 people for the purpose of stealing QQ accounts and QQ coins, a kind of cyber coin that can be purchased by real money for the purpose of beautifying the QQ blog space, by means of sending a Trojan horse software. Mr. King paid his so-called employees 5 cents RMB per every QQ account and QQ coins they stole. The case report

13. Yu Zhi Gang "The Legal Principle of Cyber Crime" Yuan Zhao Publishing Company, Taipei. 2007-3, Page 260.

14. The full name of Mr. King and other 11 defendants has not been release by the court.

did not say how many accounts and coins were stolen but one of his employees did receive 7000 RMB within a single month as payment. Thus, one can do the math on how many accounts and coins were stolen by those racketeers. After Mr. King stole those accounts and coins, he then sold all of them to another person Mr. Yue.¹⁵

Discovered by legal authority and arrested by the police, the issue then arose. On what legal reasoning should the authority prosecute them? Could QQ accounts and QQ coins be seen as a kind of property that can be protected under Civil Code and Criminal Code?¹⁶ It was submitted that the value of QQ accounts and QQ coins were uncertain and difficult to determine, although they possessed certain values, especially the QQ coins, which could be purchased with real world money. Therefore, it could not be seen as a kind of legal property that was protected under the law.¹⁷ Although it was determined by the court that the suspects did steal and that the stolen property involved in the case was not protected by the law, the court stated that the behavior from those suspects were definitely wrong and must be punished accordingly. After some thought by the court, the judge used reason based on Article 252 of the Criminal Code for obstructing people's freedom of communication. Thus, all the suspects involved in this case had been sentenced from 6 months to 1 year (which is the maximum sentence under this category of crime).

Although the case above has been settled and became one of the important precedents for this type of cyber theft in recent years, this case has actually created more problems than solving them. First of all, there has not been any difference in the sentence between stealing 10 internet accounts and stealing 10,000 internet accounts. The maximum sentence is always 1 year. However, a person who steals internet accounts and uses the private information within those accounts for gaining profit is also penalized under internet hacking. Generally speaking, the penalty for stealing internet accounts is a bit weak. In addition, because the law does not recognize internet accounts and internet coins as a kind of legal property that is protected under the law, it would not only affect the criminal sanctions for such kind of behavior but also create obstacles in respect to civil remedies and torts that the victim may be willing to take in. If you spent an arm and a leg for a particular QQ account that is made up of lucky

15. QQ Technology News "11 person found guilty by the first instance court for breaching of the freedom of communication with stealing QQ accounts," <http://tech.qq.com/a/20080214/000086.htm> 2008-02-14.

16. Civil Code and Criminal Code.

17. QQ Technology News "11 person found guilty by the first instance court for breaching of the freedom of communication with stealing QQ accounts," <http://tech.qq.com/a/20080214/000086.htm> 2008-02-14.

numbers and it gets stolen, what would be your remedies be in China? For torts, you will not have any remedies, which means you will not get your money back. For criminal law, if you are lucky enough to have your account be stolen along with many others, then the police may be willing to investigate and someone may end up in the prison. Though it might make you feel better, you may not have any substantial remedy.

Finally, the fourth type of cyber stealing is the equipment within the computer games that are tradable in the real world with real money. This problem is similar to QQ accounts and QQ coins. How do you value them? One can only have his property stolen if that property is protectable under the law and has a recognizable value. The cyber game instruments are not purchased by the players but earned by effort, time, and skill in playing those games. In fact, purchasing game equipment with money is a short cut to play the game. So, how would you recognize the value of cyber equipment from a computer game? The valuation of cyber equipment or any cyber assets are a bit like the standard of care in torts—that is, you must find something to judge against first. There are five opinions when dealing with the valuation of cyber properties:

1. According to the amount of time, efforts, and money put into gaining that cyber game equipment. In other words, whether one acquires the equipment by pure money or earned with a lot of input of time, effort, and skill, all of these factors should be taken into consideration when valuing those assets.
2. Only consider the monetary values of those cyber equipment. In other words, the more abstract elements, such as time, efforts, skills, will not be considered.
3. An objective person test, same as the first but with added consideration on how much value an “objective person” would put to acquire such cyber equipment.
4. The selling price set by the internet game company for those cyber equipment, if purchased directly from them.
5. The selling price of the thief when they resell the stolen cyber equipment to others.

Currently, based on several cases in recent years, the court seems to be leaning towards the first type of opinion: that it will consider time, effort, and money spent to acquire that cyber game equipment.

2. Case Study - Cyber Game Equipment Thief

In 2006 in Zhejiang province (浙江省), the City of Ningbo (宁波市) handled by the Ningbo district court, a case happened as someone's cyber game account was stolen. The defendant ZHANG Bin (张斌) in this case was accused of selling a particular game account known as “Heaven

1st" for the price of 4800 RMB. After he sold that account, he then hacked back into the system and stole back the particular account to himself. The plaintiff reported to the police and the defendant was arrested by the police. In the prosecutor's opinion, cyber property should be seen as a kind of immovable property that can be purchased or sold, either with monetary consideration or not. Therefore, it should be treated as a kind of property with value and should be protected by the law. Thus, the behavior of ZHANG Bin should be seen as a crime of theft under the Criminal Code. The court agreed with the prosecutor and sentenced ZHANG Bin imprisonment for one year with a fine of 5000 RMB.¹⁸

This is one of the cases that recognize cyber theft as a crime and recognize cyber equipment (accounts, equipment, status, etc.) as a kind of legal property, as long as it is tradable in the real world. However, as China is not a common law country, this kind of precedent usually serves only limited persuasive value towards other similar cases that occurred later.

IV. HACKER

The origins of the name hacker come from a group of computer engineers from Massachusetts Institute of Technology during the 1960's. They analyzed, studied and perfected the computer system. Others call them hackers.¹⁹ The original meaning of hacker was actually a name of praise. Hackers were technical people who worked for the aim of improving computer and internet systems as a whole. Just like a double edged sword, if one side works for good, the other side may work for bad. Although, hackers were working under good will, they did possess a lot of technical powers that, if misused, may create havoc towards the cyber world. The human nature is similar to a double-edged sword and some hackers may cross the line for the purpose of gaining money, power, and self-satisfaction. Though most hackers were originally good, the hackers that went to the wrong side were called "crackers." Crackers were those people who created a lot of mischief on the internet. In recent years, the line between hackers and crackers is not that clear. More and more people refer to crackers as hackers. Though hackers and crackers were originally two different groups, they have now been emerged into one. Today, when we say the word hackers, we refer to those who create havoc on the internet, such as making viruses, stealing confidential information, and crashing systems.

18. Jin Yang Wan News "Ningbo court convicts a cyber account thief." http://www.ycwb.com/gb/content/2006-01/26/content_1062508.htm 2006-01-26.

19. Ji Jing and Zhang Zhi Chao "A Study on the New Type of Cyber Criminal Behavior" Chinese Public Prosecution Bureau Publishing Co., 2012 page 121.

Currently, when we look at hackers, we can basically divide them into three different categories:

1. Hacker grouped under patriotic reasons
2. Hackers acting solo for no other reason but booting self-esteem
3. Hacker acting either in groups or solo for illegal purposes

First, let us look at the patriotic hackers. China's internet only became widespread and available to the public around 1996. Before 1996, although the internet was available, it was very expensive and only available to institutions. Around 1996, the largest internet provider, China Telecom (a state owned enterprise) (中国电信), dramatically decreased the price for internet services. It was then that the internet became widely available, which created a boom of hackers in China.²⁰ On May 1999 when the U.S. bomber mistakenly bombed the Chinese embassy in the former Yugoslavia, Chinese patriotic hackers grouped up and honed their skills. Those Chinese hackers formed an internet alliance and called themselves "The Chinese Red Hackers" (中国红客) and attacked the U.S websites and email providers. As a result, a large number of U.S email providers and internet service providers were paralyzed by those attacks. From 1999 till now, those Red Hackers became more sophisticated and skillful. They appeared whenever there were political incidents and when China clashed with other countries, such as the United States or Japan.²¹ Recently, there is a claim that some of these Red Hackers have been absorbed by the Chinese government for strategic cyber warfare purpose.²²

With patriotic hackers, their behavior is obviously illegal under Chinese law. However, it is still mostly a political matter rather than legal matter. With respect to the other two types of hackers, it is completely illegal. Therefore, let us look at what kind of law sanctions this type of behavior in China. According to the People's Republic of China Criminal Code Article 285 and 286:

Article 285: Whoever, in violation of State regulations, invades the computer information system in the fields of state affairs, national defense construction or sophisticated science and technology shall be sentenced to fixed-term imprisonment of not more than three years or criminal detention.

20. Baike Encyclopedia "The Chinese Internet History," <http://www.baike.com/wiki/中国互联网史> 2015-01-27.

21. Wikipedia Chinese "The Chinese Red Hackers," <https://zh.wikipedia.org/wiki/红客> 2015-12-12.

22. CNN News "What we know about the Chinese army's alleged cyber spying unit," <http://edition.cnn.com/2014/05/20/world/asia/china-unit-61398/> 2014-05-20.

Article 286: Whoever, in violation of State regulations, cancels, alters, increases or jams the functions of the computer information system, thereby making it impossible for the system to operate normally, if the consequences are serious, shall be sentenced to fixed-term imprisonment of not more than five years or criminal detention; if the consequences are especially serious, he shall be sentenced to fixed-term imprisonment of not less than five years.

Whoever, in violation of State regulations, cancels, alters or increases the data stored in or handled or transmitted by the computer information system or its application program, if the consequences are serious, shall be punished in accordance with the provisions of the preceding paragraph.

Whoever intentionally creates or spreads destructive programs such as the computer viruses, thus affecting the normal operation of the computer system, if the consequences are serious, shall be punished in accordance with the provisions of the first paragraph.

Based on these two articles, we get two observations. First, it does not seem to require *mens rea* when one commits the crime of hacking. This means, the prosecutor does not need to prove whether a defendant was aiming at hacking into other people's system, so long as the consequence of the defendant's behavior would be guilty under such crime. However, on the other hand, when spreading a virus, *mens rea* is required. This means intent must be proven by the prosecution. For example, it may be that one may design a particular program for the benefit of some purpose. However, if it ends up turning into a virus, spreading, and damaging many computer systems, then that person may have a defense.

With respect to the problem of hacking, there is another problem. The Criminal Code stipulated that only a person over the age of 16 years is criminally liable under the code. As computer crime is not like traditional crime that may need a lot of physical strength in able to commit such crime, cybercrime is a kind of intellectual crime that could be performed by people at very young age. The dilemma is whether it may be fair and reasonable for the legislature to lower the age for penalties to this particular type of crime. Currently, how to solve and deter the problem of underage hackers is a topic that is still hotly debated in China.

1. Case Study - Underage Hacker

In 2007, there was an underage hacker (identity withheld) who created a computer virus called "Rabbit Baby." He put that virus on his blog space. This virus was extremely aggressive and destructive. Although it

was scanned by an anti-virus software, once infected, the damaged data could not be restored. This type of virus was not made for profitable purpose but for bragging. As the virus spread widely and authority was involved with the investigation, the minor was arrested. However, based on Article 17 of the Criminal Code, he was underage and could not be criminally prosecuted. Accordingly the minor was released with no penalty.²³

V. DEFAMATION

Defamation is where a person's reputation gets defamed either intentionally or by slander or libel. Slander occurs by depleting people's reputation by images while libel occurs by words. These could be done directly or by innuendo where the information used to defame others is false.²⁴ With the requirement of defamation, those injurious words or images must be spread to the public and the meaning of the injurious substance must be relatively understandable by the public who receives it. The traditional medium for spreading such injurious substances is by newspaper, radio broadcast, magazines, and sculptures. The development of the internet took over almost all traditional mediums and became one of the most important fields of battle for defamation.

Defamation has been well developed in common law jurisdictions such as under the Fourth Amendment of the United States Constitution.²⁵ It is interesting to note that in the United Kingdom, there was no protection of privacy under the traditional English law with only some protection in the area of "breach of confidence." This has influenced the Commonwealth countries, such as Australia. In Australia, although there are no general protections in common law, since the enactment of the Privacy Act 1988 (Cth), privacy principles are now protected under the statute.²⁶ In Great Britain, it was the enactment of the Human Right Act 1998, which implemented the European Convention on Human Rights into the UK law. As the European Convention on Human Rights required privacy principles, there are now privacy principles in the UK *de facto*.²⁷

Privacy is regulated in Chinese law both criminally and civilly. As mentioned before, cyber wrongs are mostly cybercrime in China because

23. Ji Jing and Zhang Zhi Chao "A Study on the New Type of Cyber Criminal Behavior" Chinese Public Prosecution Bureau Publishing Co., 2012 page 137.

24. *Berkoff v. Burchill* and another [1996] 4 All ER 1008.

25. The Fourth Amendment did not use the word "Privacy" itself, but the concept of it appears in it against "unreasonable search and seizures. William Mc Geveran "Privacy and Data Protection Law." Foundation Press, USA, 2016.

26. Martin Davies "Torts" 4th edition, Butterworths, Australia.

27. Barbara Harvey & John Marston, "Case and Commentary on Tort," 3rd edition, Financial Times Pitman Publishing, United Kingdom.

civil compensations are insufficient for victims. Most importantly, it would be very difficult for a victim to prove his case, if the police were not involved, and usually the police do not get involved in civil litigation. On the other hand, defamation is different. There are many cases that have been successfully litigated, directly from civil litigation based on the tort law in China. While others may be sued criminally by the public prosecutor in the first instance, the victims would later use the criminal evidence for them to prove damage in a civil law suit.

Criminally speaking, the law governing this area is Article 246 of the Criminal Code, in which it stipulates:

Whoever, by violence or other methods, publicly humiliates another person or invents stories to defame him, if the circumstances are serious, shall be sentenced to fixed-term imprisonment of no more than three years, criminal detention, public surveillance or deprivation of political rights.

The crime mentioned in the preceding paragraph shall be handled only upon complaint, except where serious harm is done to public order or to the interests of the State.

In 2013, with the application of "*Interpretation of the Supreme People's Court and the Supreme People's Procuratorate on Several Issues concerning the Specific Application of Law in the Handling of Defamation through Information Networks and Other Criminal Cases*" (最高人民法院、最高人民检察院关于办理利用信息网络实施诽谤等刑事案件适用法律若干问题的解释) with 10 Articles, provided detailed guidelines for the court to determine defamation cases. The more interesting part with this interpretation is Article 2.1 in which it stipulates: any of the following circumstances of defaming another person through an information network shall be deemed as a "serious circumstance" as mentioned in paragraph 1, Article 246 of the Criminal Code - the same defamatory information is actually clicked or browsed for more than 5,000 times or is forwarded for more than 500 times.

There are a lot of discussions on how one determines whether a particular message has been browsed more than 5,000 times and forwarded for more than 500 times and the real agenda for such an interpretation as issued by the Supreme People's Court.²⁸ It is submitted that most of the recent important defamation cases has been determined before the implementation of such interpretation.

28. The New York Times, Chinese "*The statutory interpretation from the Supreme People's Court and the Supreme People's Procuratorate may further depress the freedom of speech*" <http://cn.nytimes.com/china/20130911/cc11libel/> 2013-09-11.

With tortious remedies, the main statute governing this area is the Tort Law of the People's Republic of China 2010. Article 36 stipulates:

A network user or network service provider who infringes upon the civil right or interest of another person through network shall assume the tort liability.

Where a network user commits a tort through the network services, the victim of the tort shall be entitled to notify the network service provider to take such necessary measures as deletion, block or disconnection. If, after being notified, the network service provider fails to take necessary measures in a timely manner, it shall be jointly and severally liable for any additional harm with the network user.

Where a network service provider knows that a network user is infringing upon a civil right or interest of another person through its network services, and fails to take necessary measures, it shall be jointly and severally liable for any additional harm with the network user.

This Article actually puts both the person using the network to defame others and the service provider equally liable, if the service provider knew that its client was using their service to infringe on other people's right and did nothing about it.

Regardless of criminal or torts, the problem for cyber defamation compared to the traditional form of defamation is that, first, it is anonymous. Recently, the government have been forcing people to register their real name when using the internet.²⁹ Compared with the traditional form of information medium, such as newspapers, the internet is still very much more anonymous. Since people know that they can hide their identity behind the internet, they are much more willing to speak irresponsibly. Secondly, it spreads very quickly. When someone wrote something silly in China on the internet, a person in the United Kingdom can read it only seconds later. Until 2013, there are 590,560,000 internet users in China. Thus, one can see how defamed information on the internet can not only travel very fast but also widely, as well.³⁰

With the general principle of defamation, a person may defame another person either intentionally or negligently if, objectively speaking, the

29. Baidu Encyclopedia "The Real Name System of the Internet." <http://baike.baidu.com/view/529067.htm>.

30. Sina Technology News "China has 5.91 hundred million net users and 4.64 hundred million mobile phone users." <http://tech.sina.com.cn/i/2013-07-17/14088548488.shtml> 2013-07-17.

person who was defamed has their reputation damaged. China's defamation law is leaning more towards an intentional defamation. Article 246 of the Criminal Code states, "with person who invent story who defame him." It would be difficult to invent a story without intentionally doing so. A government body or a company could not be defamed because a government body or a company does not have the right of personality based on a German Civil Law, a type of legal principle China is a part of. In other words, in China, only a natural person could be defamed. Unlike common law jurisdictions, a government cannot be defamed based on public interest but a company certainly could sue for defamation, if not injurious falsehood. The problem about company reputations in China is looked at in the next section, when we talk about cyber hyper and cyber hitman.

1. Case Study - The SONE Zue De Defamation Case

A movie director named SONE Zue De (宋祖德) and his brother LIU Xin Da (刘信达) operated a blog in Sina net, in which they disclosed private affairs of other show business people, for the purpose of getting attention. The information about other show biz people were gossip and false information, such as movie star A is having an affair and movie star B is a gay. For a while, the targeted people just ignored him, which made him bolder and bolder. On October 2008, a famous movie director Mr. Xie Jin (谢晋) suddenly passed away. Sone started to make up horrendous stories about Mr. Xie's private life. According to his blog, he accused Mr. Xie of having an inter-marital affair with another movie star Ms. LIU Xiao Qin, (刘晓庆), and having an illegitimate child together, born paralyzed in the brain. He claimed that they put their son overseas and that the son was now 21 years of age, cared for by a maid. He then used explicit words to describe their so-called son's daily life, involving the eating of human feces. Later Sone's brother LIU Xin Da published another article on his blog, suggesting Mr. Xie died because of seeing prostitutes and that he was willing to testify on such claim. In fact, all of these accusations were false and were made up by the two brothers for the purpose of gaining attention. As such, the widow of Mr. Xie sued both brothers for defamation under civil jurisdictions. The Shanghai Jinan District Court held that the two brothers defamed Mr. Xie, ordering a public apology on the internet and the public media and damages for 89,951.62 RMB and 200,000 RMB for psychological harm to Mr. Xie's widow. At

the same time, Sina net also shut down the brother's blog and refused to let them open any other new blogs in their service.³¹

This case is one of the most famous defamation cases in recent years, deterring people who tried to get attention by defaming other people. Recently in China, there is a tendency where people who want to become famous in the entertainment business must firstly gain attention from the public, regardless of whether the attention is good or bad. We will elaborate more on this when we discuss internet pornography later. However, a positive outcome of this case is that the Sone brothers disappeared from the public eye. Perhaps this is not what they were hoping to achieve when they decided to defame other in order to gain their own fame.

2. Case Study - Defaming the Government

The case study here refers to a number of cases with a similar material facts and the same issue: defamation towards the government. The material facts are that someone complains about a dysfunction of a governmental departments or government official, (usually a provincial or local government), to the relevant authorities, such as the court. When their complaint does not get the proper attention with those authorities, they put their complaint on the internet. Once the public is made aware of the complaint, the government or the official gets angry and arrests those complainants and puts them into the prison with the reason of "defaming the government." A problem with these types of cases is that the complaints are usually proven later to be true. Quite a few of these cases occurred in recent China, such as the "Ling Bo case" (灵宝案) of 2008,³² "Peng Shui Poem case" (彭水诗案) of 2007,³³ and "Cao County case" (曹县案) of 2009.³⁴ Generally, someone complained about the government on the internet based on something that was true and the government got angry, arrested, then imprisoned the complainants for defaming the government.

This kind of situation is more political than legal. It is clear that based on Chinese law, as said before, the government could not be defamed because it did not possess a right of personality like a natural person. Also,

31. West China City News, Cheng Du "Song Zu De apologised to Xie Jing's widow and said he and Liu Xin Da were sorry," <http://ent.163.com/10/0520/07/67421HDJ00031H2L.html> 2010-05-20.

32. Ifeng News "How did the problem of Ling Bo case solved," <http://news.ifeng.com/opinion/topic/lingbao/> 2009-06-28.

33. Baidu Encyclopedia "Peng Shui Poem Case," <http://baike.baidu.com/view/813180.htm>.

34. South Eastern Bulletin, Xiemen "An Investigation on the Cao County Case," <http://news.163.com/09/0727/02/5F6ON11U000120GR.html> 2009-07-27.

it is a universal defense for defamation if the so-called "defamed statements" are, in fact, true. Therefore, besides the government abusing its authority, the government did not have any standing to arrest those people. In addition, Article 41 of the People's Republic of China Constitution states:

Citizens of the People's Republic of China have the right to criticize and make suggestions regarding any State organ or functionary. Citizens have the right to make to relevant State organs complaints or charges against, or exposures of, any State organ or functionary for violation of law or dereliction of duty; but fabrication or distortion of facts for purposes of libel or false incrimination is prohibited.

The State organ concerned must, in a responsible manner and by ascertaining the facts, deal with the complaints, charges or exposures made by citizens. No one may suppress such complaints, charges and exposures or retaliate against the citizens making them.

Citizens who have suffered losses as a result of infringement of their civic rights by any State organ or functionary have the right to compensation in accordance with the provisions of law.

Accordingly, the government's behavior was not only contravening the normal legal principles but was also unconstitutional. It is true that with most of these cases that most of the arrested people were released, where some were even compensated for wrongful detention. The only problem was that the compensation was not proportional to the ordeal they went through. In the "Ling Bo case," the defendant, Mr. Wang, was arrested and imprisoned but the compensation for his wrongful arrest was only 783 dollars RMB (around \$25 USD).

VI. CYBER HYPER

The practice for cyber hyper is currently legal in China but may be morally questionable. Cyber hyper means people create a publicity stunt on the web for achieving a particular purpose, usually aimed at making someone or some company famous. The motto for those cyber hypers is that to be able to get one person famous, the person must gain public attention first, regardless whether that attention is a good or bad. In fact, bad attention, unless illegal, will always makes the public remember the person more. Thus, those cyber hypers are always pushing the matter close to the legal borderline, stretching the public's moral nerve to its limits.

The most famous cyber hyper case is the case known as the "Furong Sister's" case (芙蓉姐姐). From August 2002 to early 2004, there was an

ID named "huobingker" registered in the Peking University (北京大学) Weiyen BBS (未名 BBS). The girl continued to send sexually suggestive pictures to the forum, claiming she was the most beautiful lady in China. Later she posted her pictures onto the Tsinghua University (清华大学) BBS (水木清华) and a few other general forums as well. She successfully stirred up a heated debate on her behavior and received the attention she wanted. She began to engage with show business agencies, entering the show business world, and becoming an actor and advertiser. At one stage, she was the most famous person on the Chinese internet (even Taiwan and Hong Kong noticed her), and at the peak of her fame around 2005, her phenomenon was actually reported by "Time Magazine" and various other international news medias.³⁵ Although her behavior was not illegal, according to the Chinese government's eyes, it did not create a positive image for China. As the Propaganda Ministry (中国共产党中央宣传部) kicked in, the whole phenomenon died out quickly. However, the Furong Sister had already successfully entered the entertainment industry. Today, she is still working as an actor, although not as successful.³⁶

The problem with the Furong Sister phenomenon and how it could have been possible was only recently been made clear. Unlike what people originally thought, that some girl posted her picture around the internet to show off and that the whole matter just got out of hand, the phenomenon was, in fact, a precise project designed by a cyber-hyper know as Mr. CHEN Mo (陈墨). An internet advertiser and planner, Mr. Chen ran an internet advertising agency. Furong Sister was his most successful product in which every step was carefully calculated and planned.³⁷ Since the Furong Sister phenomenon, Mr. Chen became very famous, bringing a lot of business into his firm.

The Furong Sister phenomenon was the first and most famous cyber hyper case. After the Furong case, many similar cases appeared such as "Hooligan Swallow" in 2005, "February Girl" in 2006, and "The Most Pretty Cleaner" in 2008. There are many more of them and they all are pushed by cyber hypers for the purpose of making their products famous. Is the behavior of cyber hypers illegal? On August 2013, the Chinese government arrested two famous cyber hypers known as "Li Er Chai Si" and

35. Sina Blog "Furong sister in my heart," http://blog.sina.com.cn/s/blog_4b55310901008vvp.html 2008-03-18.

36. Wikipedia "Sister Furong," https://en.wikipedia.org/wiki/Shi_Hengxia.

37. Tiexue Net "This is how the cyber hyper Chen Mo made Furong sister famous," http://bbs.tiexue.net/post2_3246191_1.html 2008-12-17.

“QIN Huo Huo” for spreading rumors and defaming public figure.³⁸ This is interesting because the concept between “cyber hyper” and “spreading rumors and defame public figure” are actually two different things. This case itself still does not provide us with a clear picture of the legality on the behavior of cyber hyper.

A. Traditional Order and Value

Where is the fine line between cyber hypers and cyber advertisers? Does it look like they are trying to achieve the same result? Perhaps the division is not a legal one but a moral one and should be dealt with a “Traditional Order and Value” (公序良俗), which was originally a concept derived from Roman law, now incorporated in the general rules of civil law in Japan, France, Taiwan and Mainland China, etc.³⁹ Traditional order and value requirement may arise in practice under Chinese inheritance law when dealing with wills. There are many instances, for example, of the husband dying and leaving all of his property to his mistress, instead of his widow and children. The most famous case happened in 2001 Luzhou City (泸州市). A man lived with his girlfriend for many years and even had a daughter. The man never divorced his estranged wife. When he died, he left all his property to his girlfriend. His legal wife and children contested the legality of his testamentary, which was later upheld by the court under the reason that it was against the tradition order and value. The testator’s girlfriend got nothing.⁴⁰ This case had a lot of debate, even today. A scholar suggests the verdict of that case was not a fair one and that the testator’s girlfriend should have at least received a portion of the property. There are other kind of testamentary, such as the testator leaving all the property to his or her care taker instead of their spouse or ken. This kind of testamentary has a lot of debate towards it. The most famous case occurred in 2001, in Hangzhou City (杭州市), where an old man left all his property to his employed care taker (a young girl) instead of his daughters. This was upheld by the court as a legitimate testamentary.⁴¹

38. Baidu Encyclopedia “Li ER Chai Si” http://baike.baidu.com/link?url=H04qL_UWRsXhuwrjo9az6F676l2kBE8e8dquEMIVYT06LiHfEm5VvUTqcGldhIGR21SwF6kFUVyYB7GiV4l.6tNGF3zxXc_M0rZrvUkNW3cO.

39. Baidu Encyclopedia “Traditional Order and Value.” http://baike.baidu.com/link?url=c6XD5SI0vO5_qkjhIXehyMVjFPK2c0LgE8wgZPJqkbn_O06otKcMjgD911Z9e3ruxBqPjrvFI2qjV7jtWAZM2t8y5NYX6nSnN-gQTlwyN0OsrzdFcIscQbqptEeZyO.

40. Yang Li Xin, Yang Li Jun “A rethink toward the compulsory portion under inheritance law.” <http://www.acla.org.cn/html/lilunyanjiu/20140208/14850.html> All China Lawyer Association, 2014-02-08.

41. Rai Guo “Our Current lack of Testamentary Succession System with Perfect - to up to two typical inherit case thinking.” <http://www.docin.com/p-1459875945.html> 2011-6.

We are not dealing with inheritance law here but the author thinks the concept of this "Traditional Order and Value" can also apply to cyber hyp-ers because the behavior of cyber hyper, although not illegal, depends on what kinds of drastic actions people take to draw people's attention. Some of their behaviors, such as being half naked in a populated place, may not be against the law *per se* but are certainly not in accord with standard values.

VII. CYBER HITMAN

Cyber hitman means people or group of people who defame or falsely accuse a person or company for the purpose of destroying their reputation for political or commercial reasons. This is very similar to the situation of malicious falsehood under the common law defamation. However, as mentioned earlier, China so far does not have remedies for defamation against the company, regardless of business reputation or not. It is important to note that although China does not have the civil remedies for malicious falsehood, there is Article 221 of the Criminal Code which stipulates a crime of disrupting market order. According to Article 221 of the Criminal Code:

Article 221 Whoever fabricates stories and spreads them to damage another person's business credit or commodity reputation, if heavy losses are caused to the person, or if there are other serious circumstances, shall be sentenced to fixed-term imprisonment of not more than two years or criminal detention and shall also, or shall only, be fined.

1. Case Study - The Yili QQ Star Milk

On July 14th, 2010, there was an article published on various newspapers about "deep sea fish oil usually possessed health problems." On July 27th, 2010, there was an ID named "Young Mother" who appeared on a lot of internet forums, asking the same question: "My baby just weaned, is Yili Dairy QQ star milk (A branded milk in China) (伊利 QQ 星) safe for baby to drink as alternative to breast feeding?" Someone replied, "You did not know? Yili's QQ Star milk actually had the ingredient of deep-sea fish oil, it will make your baby sexually premature, do not let your baby drink that milk." Then later, someone further stipulated that his son, because of drinking Yili QQ star milk, was now growing facial hair. These kinds of statements appeared hundreds of times in various forums.

As the result of the negative publicity, all of the parents were shocked and the sale of Yili QQ star milk dropped like a falling stone.⁴²

Yili Dairy (伊利乳业) reported the incident to the police. After police investigation, it was discovered that the whole matter was planned by AN Yong (安勇), an employee of Mengniu Dairy (蒙牛乳业) (product manager) who was a major competitor of Yili Dairy, together with Bo Si Zhi Public Relation Company (北京博思智奇公关顾问公司), which was the PR company who worked with Mengniu Dairy. As a result, AN Yong, and HAO Li Ping (郝历平), ZHAO Ning (赵宁), and MA Yeh (马野) of the Bo Si Zhi Public Relation Company were all arrested accordingly.

In the Yili case, the people involved were arrested based on Article 221 of the Criminal Code. However, there was no evidence to suggest that Mengniu Dairy Company actually knew that its product manager, AN Yong, was involved. Thus, it was seen as the independent behavior of AN Yong. The Mengniu Dairy company escaped liabilities. Currently in China, there are a lot of suggestions that there should be an Article for malicious falsehood being implemented into the Chinese tort law, since this kind of behavior should be de-criminalized with more emphasis on its civil liabilities, in which a large amount of damages may be the key to discourage these kind of practices.

VIII. CYBER PORNOGRAPHY

According to Article 367 of the Criminal Code:

For the purpose of this Law, pornographic materials refer to obscene books, periodicals, movies, video-and audio-tapes, pictures, etc. that explicitly portray sexual behavior or undisguisedly publicize pornographic materials.

Scientific works on human physiology or medical knowledge are not pornographic materials.

Literary and art works of artistic value which contain erotic contents shall not be regarded as pornographic materials.”

The Criminal Code in this regards are the mother law regulating this area. There is a further interpretation provided by the Supreme People's Court: *“Interpretation of the Supreme People's Court and the Supreme People's Procuratorate on Several Issues concerning the Concrete Application of Law in the Handling of Criminal Cases of Making, Reproducing,*

42. Baidu Encyclopedia “The An Yong Incident.” http://baike.baidu.com/link?url=619tUN-Nlt_160ahS78chxcFwX0K3M8SzcNc6BMJ_ZdOHgxDoh5ncGAXHNUMYKCQE131vdaxwJE-RnYbeSmbcq.

Publishing, Selling and Spreading Pornographic Electronic Information by Means of the Internet, Terminal of Mobile Communications and Sound Message Stations" 2004. This interpretation mainly deals with providing pornographic materials via internet for commercial purpose.

The above two laws are legal reasoning that cracked down several internet pornographies recently. The most recent internet pornography crackdown was in 2014 organized by the "Anti-Piracy and Pornography Working Committee" (扫黄打非工作小组办公室), a governmental working group, the "Office of National Internet Information" (国家互联网信息办公室), the "Ministry of Industry and Information Technology" (工业和信息化部), and the "Ministry of Public Security" (公安部) in co-operation with each other for the purpose of cracking down on piracy works and pornography.⁴³

Pornographic materials consist of articles of words, pictures, films, etc. There are a huge number of materials providing the description on what can be seen as pornography, thus the author will not put too much emphasize on this. Generally speaking, you will know on its face whether it is pornography or not. The interesting question here is whether China allows this kind of materials to be freely circulated. At this point it is important to note that when we talk about internet pornography, it is different to cyber erotic services. Cyber erotic service, which may involve prostitution, is actually using the internet as a means of communication or advertisement, for the purpose of providing services. This situation in fact is just like swapping the traditional yellow pages to internet catalogs. Whether this action is legal or not depends on the jurisdiction of the country on whether prostitution is legal or not. Currently, prostitution is illegal in China, thus cyber erotic service is also illegal, as well.⁴⁴

The problem with internet pornography is that it is very easy to get access, unlike the traditional means of supply where one can put certain restrictions on who can access those materials. For example, in Australia, underage people are not allowed to enter certain kinds of bookshops or purchase certain rated films. On the internet, although it is possible to establish a classification system or a parenting software individually, the nature of the internet makes it difficult to totally restrict underage access. This is the main reason, provided by the Chinese government, for a blanket ban on pornography materials: to protect underage children.

43. Xinhua News Agency "The 2014 action on the elimination of pornography and illegal publications on the net," <http://www.xinhuanet.com/legal/shdf/2014-01-19>.

44. Decision of the Standing Committee of the National People's Congress on the Strict Prohibition Against Prostitution and Whoring, 1991.

It is a fact that Chinese society is much more open than during the 1980's when open policy was just implemented. Thus, people are much more tolerant with this kind of material. As such, there was always a debate on whether pornography materials should be banned at all or at least partly lifted, if the age classification system could be established and implemented. The internet is a world wide web and it does not have a true border. Therefore, even if China has the toughest ban on such kinds of materials, a lot of them still manage to hop over the Chinese great firewall from Japan and the United States.⁴⁵ One indication of this is one Japanese adult video actor, Aoi Sora (AV 女优 - 苍井空), who became a celebrity with some 400,000 Chinese fans. The simple logic is, if one did not see her adult film before, how does one become her fan?

Thus, generally speaking, when we talk about the cyber pornography problem in China, we should really divide up the problem into two parts: the providers and the users. In terms of the providers, they can be divided into domestic providers and overseas providers. In the early days, the domestic pornography providers were using pornographic materials on their website to attract viewers in order to sell advertisements. They later discovered that selling pornographic materials or organizing club memberships were much more profitable. As a result, many turned into cyber clubs, selling memberships for profit.⁴⁶ This kind of domestic provider-ship has been cracked down in recent years and very few exist anymore. Some of the surviving website masters moved their web server overseas, mostly to the United States where this kind of website could legally exist (unless it is pornographic materials concerning an underage person), to avoid the crackdown. These are now considered overseas providers due to the problem of the Chinese great firewall. Rarely will Chinese people directly go over to the pornographic websites that are run overseas domestically and not aimed at Chinese users. In addition, these overseas Chinese pornographic websites will actively find ways to overcome the Chinese great firewall, allowing domestic Chinese access. Currently, few of these overseas Chinese pornographic websites are still operating strong due to their effort. Chinese users are able to watch almost every new Japanese adult video produced within a month, in China, sometimes for totally free!

Now let us turn to the users of cyber pornography. Is it legal to watch cyber pornography privately? If not for commercial gaining purpose, currently there seems to be no law suggesting that one cannot watch those

45. Yu Zhi Gang "The Legal Principle of Cyber Crime" Yuan Zhao Publishing Company, Taipei, 2007-3.

46. The Chinese People's Net "Eliminate cyber pornography and return a clear sky back to the net," <http://it.people.com.cn/GB/8219/35192/> 2008-01-23.

materials in private circumstances. Of course, one cannot watch these materials in a public place or in a public office but those are behaviors prohibited by other means of law, such as public order or sexual harassment law, which is the normal practice for countries like the United States where cyber pornography is legal. Thus, it is fair to say that in China, watching cyber pornography may be morally questionable but not legally forbidden. However, is that always the case?

1. Case Study - Watching Pornography in Private Dwelling

On December 31, 2002, in Shanxi Province Yanan City (陕西延安), there was a couple watching pornographic movies at home just before the 2003 New Year. For some reason, the police noticed that they were watching "illegitimate stuff," (there were suggestions that someone reported them to the police). The police busted into their door and arrested the couple. Later the husband was put into detention. The only problem was that the police could not find a reason to charge the husband, as every law in China in this area only suggested that one could not sell, duplicate, transfer such movies. None of those laws expressly indicated that one could not watch them. There was a huge debate about this. Finally after a few days of detention, the husband was released and the local police department apologized to the couple.⁴⁷

This case was a very famous case and an important precedent as well. Today in China, watching pornographic movies at home is a bit like the legal arrangements back at the Prohibition era in the United States under the Volstead Act, where one could not produce, sell, transfer, supply but could drink a bottle of whiskey at your home.

Now we know that watching pornography at home may be alright but what about downloading cyber pornography? Based on the 2004 interpretation from the Supreme People's Court, one is not supposed to "reproduce" pornographic materials. Is downloading pornographic films or pictures an act of reproducing? This is very ambiguous indeed and much has been recently debated about this matter in China. Most of the intellectuals lean towards the thought that even if downloads are a kind of reproduction, reproduction for private use does not contravene the law. It is however important to note that in recent years, a few people have been fined by the police for downloading pornographic materials on the internet. However,

47. Sina News Center "From the husband and wife watching pornography video at home incident, citizen's privacy right are finally being protected," <http://news.sina.com.cn/s/2003-01-05/0921862639.shtml> 2003-01-05.

these situations are hotly disputed without any definitive conclusion.⁴⁸ There is actually a joke in China which states that if downloading pornographic material is illegal, then most of the web users would be arrested.

Downloading pornography materials may be all right with the law. However, what about uploading? Uploading is totally different from downloading. It is clearly illegal, as it is specifically forbidden by the 2004 interpretation from the Supreme People's Court as a form of "spreading pornography materials." Indeed, quite a few cases already exist, as people uploading pornographic materials for all sorts of reason end up being arrested.⁴⁹ Thus, uploading pornographic materials is definitely illegal. But what if one did not intentionally upload these materials but it was uploaded automatically due to software problems or design?

2. Case Study - Li Zhong Rei Drug and Rape Case

This case did not happen in Mainland China but in Taiwan. In 2012, there was a guy named LI Zhong Rei (李宗瑞), a rich second generation whose whole aim in life was to drink at a pub and take girls back home. After taking the girls back home, he would drug them and film having sex with them while the girls were unconscious. He collected those films, stored it in his computer, and later used it to brag to his friends. About 30 girls fell prey to him. It was on July 2012 that two sisters discovered they had been drugged and raped by Li, bringing this case to police investigation. The whole matter was discovered and consequently Li was charged by the prosecutor. Li was charged under the Taiwanese Criminal Code with rape and interference with the right of private secrecy among others things. Due to the fact that his crime was particularly serious, as more than 30 victims were involved, he was then sentenced to 30 years of imprisonment.⁵⁰

The area that we are concerning is actually not Li's case itself but the film he made when he drugged and had intercourse with the 30 girls and what happened afterwards. After he made those films, he sent the video to his friends. Some of the films ended up being released. When he was charged and arrested, someone actually released all the films to the public, which contained some 29 GB of space with 60 something girls in the film.

48. Net Easte News "Is watching pornography video on the internet illegal?" <http://news.163.com/special/0001135D/changnkong1986.html?1222235436901> 2008-09-18.

49. QQ News "A man upload 62 pornography movies on the net within 3 month, but did not know it was illegal while he was being arrested," <http://news.qq.com/a/20130320/000008.htm> 2013-03-20.

50. Wikipedia, Chinese "The Li Zhong Rei sexual assault case," <https://zh.wikipedia.org/wiki/李宗瑞性侵害案>.

Some of the girls, however, were filmed with consent and was thus not illegal. Although the authorities declared that the downloading of such materials would be illegal under criminal penalties, such as interference with the right of private secrecy under the criminal code, human nature and curiosity caused people to download these films with P2P software.

Downloading such materials is usually not illegal, which is debatable but still in practice is seldom prosecuted. However, uploading them is definitely illegal in Taiwan. The design for a P2P download is that once when you are downloading, you are automatically uploading, as well. As a result, 12 downloaders were arrested for the reason of uploading those films to the web.⁵¹ Now the question is, for prosecuting the upload, is subjective intent required? It seems to be very much debatable and that those 12 arrestees should have a defense based on the lack of subjective intent. They were arrested under criminal sanctions, which means *mens rea* or “subjective intention” under the civil law system must be proven. With the way of operation of the P2P software, if you are only downloading, although uploading at the same time, it is automatically done and cannot show your own intent of uploading it. However, in this case no one seemed to be raise this question as a defense and later all of the 12 arrestees were fined and no one complained about the legitimacy of their arrest, which was quite unfortunate, indeed.

Finally, although not cyber pornography *per se*, cyber hypers who try their best to get famous with all sorts of publicities on the web, regardless of if those publicities are negative and positive, are similar. Recently in China, fame seekers will take one step further than cyber hypers and put their sexual films or photos onto the web in order to make themselves famous overnight. This phenomenon began with the case known as “Shou Shou sex films (兽兽门事件)- Di Ling (翟凌)”⁵² in 2010 and the “Uniqlo sex film incident” (优衣库性爱视频事件) in July 14, 2015. The people involved (usually female) always claimed that they were the victims of people attacking their privacy, such as hacking into their cell phones or computers. However, many believed that they were actually hyping themselves in order to become famous. The problem is that with this kind of behavior, it is usually very difficult to prove whether or not they deliberately put their sexual photos or films onto the internet or whether they were the victims of ill intent, with their cyber equipment really stolen. This kind of behavior may not be a cybercrime but is certainly a kind of cyber wrong.

51. South Eastern Commerce News “12 person being arrested for downloading Li Zhong Rei sex videos,” <http://news.e23.cn/content/2012-09-11/2012091100300.html> 2012-09-11.

52. Wikipedia, Chinese “Di Ling,” <https://zh.wikipedia.org/wiki/翟凌>.

This is the area that relevant authorities must find ways to deter this kind of practice from getting copied by many.

A. Naked Chatting and Cyber Sex

In addition to this, the latest phenomenon in China is known as “naked chatting” (裸聊), in which some people organize a website and employ young girls in different chatrooms. The user buys cyber presents in that chatting website. The more the user pays (buy presents), the more the girls will explicitly chat with them by taking off their clothes. If the user pays them top dollars, they will chat naked and even perform some kind of sex act to satisfy the sexual fantasy of the user.⁵³ This is, of course, the typical example of “cybersex.” Currently, all forms of naked chatting and cybersex (unless done privately between two consenting adults without any financial considerations) are strictly sanctioned by Chinese authorities, including Taiwan. But then again, there is an old Chinese saying, “the priest climbs a foot, the devil climbs ten” (道高一尺魔高一丈). Illegal or not, as this is a relatively simple and lucrative business, the author believes this phenomenon will never be totally eliminated but grow larger in scale.

On the other hand, can one really say naked chatting or cybersex is a form of cyber wrong? It really is not much different compared to the traditional forms of prostitution, basically identical to “phone sex” or “call girls,” which existed even in the 1970’s. The fundamental difference is with the improvement of cyber technologies, this kind of traditional form of prostitution becomes more diverse through the medium of the internet. Thus, the author believes that the central question about issues of cybersex or cyber pornography is not “cyber” itself but whether you see pornography and prostitution as legal. Once the argument enters this area, it becomes a valuable argument. It seems to be just like abortion, euthanasia, and marijuana in which you can never find a clear cut answer. Currently in China, beside cyber pornography, cyber gambling is another area that has the same issues. There again, the problem does not lie about the cyber aspect. The argument is whether gambling should be legalized, at all.

IX. THE TAIWANESE FIRST COMMERCIAL BANK HEIST

After looking at many types of traditional forms of cyber wrongs, let us look at a recent case in Taiwan. This case has all the elements of tradi-

53. Yu Zhi Gang “*The Legal Principle of Cyber Crime*” Yuan Zhao Publishing Company, Taipei, 2007-3, Page 262.

tional cybercrime such as cyber theft, phishing, and Trojan horse implementation. But there was another step where the criminals, like magicians, actually made an ATM machine spill money from thousands of miles away in Russia.

A. Background

On July 10, 2016, 5:30 at dawn, after a typhoon storm, a man with a face mask and black striped hat stood in front of an ATM machine, which belonged to the Taiwanese First Commercial Bank's Jilin branch at Siping Street. Amazingly, without any bankcard or password and without even touching the ATM itself, the cash continuously flowed out of the machine, like some magician putting a spell on the machine. Around the same time, there were 41 ATM machines belonging to 22 First Commercial Bank branches in Taipei and Taichung, which all together spit out \$83,277,600 New Taiwan Dollars (NT), equivalent to around \$2,629,376 USD. What amazes people was that the person receiving the cash only spent a few minutes at each of the machines before bagging more than \$2 million cash into their backpack. Based on the image from the security cameras, the thieves seemed to be a group of 16 to 17 people attacking the ATMs around the same time, without operating the machine in any way but possibly gaining control of the machine beforehand with some sort of "connecting device," possibly from their smartphones.⁵⁴

The unnatural spitting of cash was witnessed by bystanders, as they immediately reported it to the police. The First Commercial Bank immediately checked the cash inventory in their ATM machines across all branches and realized there were 41 ATM machines across Taiwan that had an abnormal cash-out situation. Once the seriousness of the situation was discovered by the First Commercial Bank, they reported it to relevant authority. As such, both the Taiwanese police and Investigation Bureau from the Taiwanese Ministry of Justice Investigation Bureau (MJIB) immediately got started with the investigation. With the initial investigation, all the thieves collecting the money were foreigners and Caucasian in appearance with around 16 to 17 people collecting from the ATM machines, at roughly the same time. Judging from similar precedents around the world, as this had happened to Japan and Thailand before, this probably was another work done by the Russian Mafia syndicate. Many questions were raised. How could they control the ATMs and instruct it to spit money without even operating or even touching the machine? If

54. Huang Yan Cai "The Path which Hackers hank into the First Commercial Bank" <http://www.ithome.com.tw/news/107294> 2016-07-25.

smartphones were the remote control devices for the job, how and by what means would it be possible to achieve this result?⁵⁵

Taiwan is an island full of close circuit televisions (CCTV). With a detailed analysis of the footage from those relevant CCTV's from First Commercial Bank, a suspect car was identified by the investigators (police and MJIB). By tracing the number plate, it was identified as a rental car. From the rental car company, the identity of the thieves was identified a few days after the incident. These people were indeed from Russia and/or Eastern European countries. However, some of them already left Taiwan the day after the incident occurred. One strange situation intrigued investigators: NT\$83 million was not a small amount of money in terms of size and weight but according to the CCTV footage from the airport, no one brought a large suitcase. All of them only had cabin luggage when they left the country. How did they take their trophy money with them, ultimately their purpose for stealing the money?⁵⁶ In another words, they either did not take any of the trophy money or only took a small amount of trophy money with them when they left Taiwan.

B. Where Did the Money Go?

Investigators believed that the stolen money was still be in Taiwan or at least in the hands of other group members who were waiting for the right moment to transfer the illegal funds overseas. In another words, this Russian crime syndicate was divided up into different teams or groups, with each team responsible for only a part of the whole business. The person caught on the CCTV who was collecting money was only responsible for cash collection. Once they finished their job, they left the country immediately. There must have been another team member from the same syndicate coming into or remaining in Taiwan who handled the transfer or remittance of the illegal cash to finish up the job. With this theory in mind, the investigators immediately began to watch out for any suspect from Russia and/or Eastern Europe entering Taiwan or remaining in Taiwan at around the same period of time. Through various channels, they started to contact both the legal financial institutions and "underground money wiring companies" to let them know the seriousness of the situation to warn them to refrain them from taking on this "business" for this group of people. Especially with the underground money wiring companies, although they were not legal, they existed in Taiwan for a very long period of time.

55. *Ibid.*

56. United Daily News, Taiwan, Editorial Department "It happened so dramatically - Understood the First Commercial Bank case in one go" <https://udn.com/news/story/10027/1823435>, 2016-07-21.

They are especially popular with business man transferring money into and out of Mainland China (as transfer money from Taiwan to Mainland China via official channel may be time consuming and involve massive red tapes). Since the underground companies did not want to have any direct conflict with the Taiwanese authorities, they decided to cooperate with Taiwanese authority, refraining from taking on this money laundering business for this group of people.⁵⁷

C. The Suspects Arrested

After thorough investigations from various channels, the investigator identified three possible suspects, one of which was Andrejs Peregudovs from Latvia. He was among the group of people who first entered into Taiwan and remained in Taiwan until the incident was complete. Niklae Penkov from Moldova and Mihail Colibaba from Romania arrived to Taiwan on July 16th, a day after the incident occurred. These three people were trying to contact underground money wiring companies to transfer the stolen money overseas. However, due to the warnings from authorities, no company dared take on their business. Therefore, these three people entered into a situation where they got a large amount of cash with no way to transfer it out of the country. As such, they tried to find a place to hide the cash while figuring out a means to transfer out those funds. As the police had blocked almost all possible channels for them to transfer out their cash, they became desperate and decided to hide the money at a rubbish dump in Taipei's Neihu District (內湖區).⁵⁸

Andrejs Peregudovs was the first person arrested by the Taiwanese authority in Taiwan's Yilan County (宜蘭縣) in July 18, 2016. According to the report, he went to a local restaurant and ordered sweet and sour fish, which is a dish only a foreigner would order at this restaurant. This was witnessed by an off-duty police officer. Because this restaurant was not a place frequented by foreigners and no locals would have ordered the dish, this immediately raised alarm. After he left the restaurant by bicycle, heading south towards Hualien County (花蓮縣), the off-duty officer contacted the local police and had Andrejs Peregudovs arrested. Andrejs later confessed he was trying to find a fishing boat, because these two counties were port counties, to take the money out of the country by a smuggling boat.

57. SETN News (三立新聞) "The Heist has become too publicized, the underground money wire companies refuse to take the business even with a 70% commission! <http://www.setn.com/News.aspx?NewsID=165462> 2016-07-18.

58. Jason Pan "East European trio indicated over First Commercial heist <http://www.taipeitimes.com/News/front/archives/2016/09/14/2003655108>. Taipei Times 2016-09-14.

Of course it was not an easy for a foreigner to find a contact for a smuggling boat in Taiwan, as there is a very good coastguard system. Later the same day, the other two suspects Niklae Penkov and Mihail Colibaba were arrested in a luxury hotel in Dazhi District (大直區).⁵⁹

Due to their arrest, most of the money stolen from the First Commercial Bank was recovered, as NT\$60,240,000 (1,910,501 USD) were found in the hotel room of the three suspects above. Two days later, an additional NT\$12,630,000 (400,558 USD) was recovered in the rubbish dump, mentioned earlier. Also, an old man Mr. Ke (柯姓老翁) reported to find an additional NT\$4,541,200 (144,023 USD) near the original location of the rubbish dump. Thus, out of the NT\$83,277,600 lost cash, NT\$77,450,000 was recovered, with around five million NT lost and presumably taken away by the first group of thieves when they left the country. With 16 or 17 people with light luggage, five million NT were feasible to take out. This means most of the money stolen from the First Commercial Bank ATMs were recovered by the Taiwanese authority (mainly the police). Thus this case was declared by the Taiwanese police as officially being solved. The group of criminals, with members from six countries (mostly from Russia and Eastern Europe), committed similar acts around the world and stole roughly more than USD\$95 million.⁶⁰ However, this case was only cracked by the Taiwanese police. This is not only a rare occurrence but it also indicates that the Taiwanese police had an advantage in cultivating relationships with different parties, which may have helped them handle this type of special and technological case.⁶¹

It was fortunate that this case was solved and that the criminals were arrested, at least some of it. However, a lot of questions remained unanswered. How it was possible that those criminals made the ATMs spill cash without even physically touching them? There are two possibilities. One possibility is that this was an "insider job" where there may have been someone inside the First Commercial Bank to cooperate with this Russian syndicate. The other possibility is that it was done by very clever cyber criminal who used some way or ways to remotely control those ATM machines. Although ATM machines are not 100% criminal proof, it

59. Apple Daily News, Taiwan "The First Commercial Bank reclaim NT60,000,000. Andrejs said he came to Taiwan to repay debt, and once this job done, he will be paid USD\$10,000." <http://www.appledaily.com.tw/realtimenews/article/new/20160718/910140/> 2016-07-18.

60. United Daily News, Taiwan. Editorial Department "It happened so dramatically - Understood the First Commercial Bank case in one go" <https://udn.com/news/story/100271823435>, 2016-07-21.

61. *Ibid.*

has been widely known that it would be very difficult to hack into the ATM system, gaining control and forcing them to spit out money.

D. Ministry of Justice Investigation Bureau, Cyber Forensics Laboratory

Once this incident happened, the Taiwanese police was active in investigating and catching those suspects who may have been involved in this case but still remained in the country. The MJIB was on the other hand busy in figuring out how it was possible that the ATM could be made to spill out cash without physical control. Both the possibility of insider job and cybercrime were investigated at the same time. Although initially the prosecutor refused to rule out the insider scenario, this was later ruled out. Thus, this paper will not focus on MJIB's initial effort on investigating the possible insiders, as this will be another area of focus in criminal activity. The other possibility of course was the cybercrime scenario, which was later proven to be the case when this case was cracked by the Taiwanese authority. The cybercrime investigation was handled by the MJIB Cyber Forensics Laboratory (CFL) (法務部調查局資安鑒識實驗室). Immediately after the incident happened the CFL experts started to work on this case towards cybercrime direction, focusing on the ATM machine. First of all, the ATMs that spilled cash were removed from the scene and sent to CFL for analysis, 41 altogether. According to their hypothesis, the only way that this kind of scenario could occur would be some kind of malware that invaded the ATMs controlling system and took over the ATM machine. But with their initial investigation, they could not find any malware in the ATM system. But with their efforts, on July 19th, which was only the next day after the incident occurred, the CFL discovered three possible types of malware that could be hiding in the ATM controlling system.⁶²

The MJIB said the machines were infected with three different malware files that instructed them to "spit out cash" and another sub-malware that would be activated to delete malware once they completed the task, to clean out evidence of the crime. The sub-malware was known as "cleanup.bat." It would work though the encrypted internal delete tool "sdelete.exe" to delete any evidence of the malware in the ATM system. Thus those hackers could come, attack, and go without any trace of their track. The only reason the CFL could figure out the existence of the three malware was because one of the ATM being attacked had a malfunction in the cleanup sub-malware. But these three types of malware did not possess the ability of far-end online engagement. This means that these types

62. Huang Yan Cai "The Path which Hackers hank into the First Commercial Bank" <http://www.ithome.com.tw/news/107294> 2016-07-25.

of malware could not remotely control the ATMs via Command and Control Server (C&C), like many hackers usually do. In order to achieve the result of the case at hand, it had to have been done manually at far end. Therefore, the CFL experts believed the hackers broke into computers within the First Commercial Bank by sending "spear phishing emails," which was a kind of phishing but more aggressive than the normal phishing emails. Once computers inside the First Commercial Bank got infected with the malware, it was possible to command those ATMs to spill cash even without physical contact.⁶³

After checking the online records from the internal net of the First Commercial Bank, it was discovered that on July 9th that there was a large amount of online engagement from First Commercial Bank's London branch towards its ATMs in Taiwan. The system with the large amount of online engagements was done through the "Telephone Recording Server" of the First Commercial Bank's London branch. It was strange as First Commercial Bank's London branch did not offer any ATM services and therefore did not need to get online with the Taiwan ATMs and should not have any record accordingly. Therefore, it was inferred by the CFL investigators that the London branch was the hacking point by the hackers and after hacking into the London branch's server, they then used the server as the jumping board to attack back into the head office of the First Commercial Bank in Taiwan. This inference was later proven by the CFL investigators as they further investigated the case and was later admitted by the suspects when they was being arrested.⁶⁴

E. The ATM Machines Itself

Another problem may point towards the problem of hardware, that is, the brand of the ATMs. The ATMs spitting money in this case was the "Pro Cash 1500 model," manufactured by a German company, Wincor Nixdorf. After the incident, Wincor Nixdorf, although cooperating with the First Commercial Bank and the Taiwanese authority, said they had no evidence to suggest that the malware was introduced into the network by the ATMs themselves. This was later proven to be the case by the CFL investigators. However, some expert suggested this model of ATM was a bit out of date and could easily be purchased on the internet to give criminals practice on how to crack them.⁶⁵ Although in this case the ATMs itself may not have been directly linked to the result of spitting money for the

63. *Ibid.*

64. *Ibid.*

65. Huang Yan Yeh, "A disclosure on the 4 banking system safety - why a closed ATM system is not safe" <http://www.jthome.com.tw/news/107306> 2016-07-25.

thieves, on a news briefing on July 18th, the chairman of the First Commercial Bank Mr. CHAI Qing Nian (蔡慶年) declared that they would replace all the Wincor Pro Cash 1500 ATMs with newer ones.

It has been suggested that many of the Taiwanese ATMs used a closed system framework known as the Systems Network Architecture (SNA). The ATMs connect directly through SNA to the bank's main system in order to determine and process customer's banking details and instructions on deposit or dispensing money. When the ATM connected with the SNA during the transmission, every process would be encrypted. Thus, in theory, the structure should have been a totally closed system and should have been failsafe. However, was it really so? If the ATM system was a totally closed system, then whenever the system needed update, it could not be updated remotely but be done by engineers manually by inserting a CD or USB disk on every machine itself. In another words, this could be time consuming and inconvenient for the Information Technology (IT) department of any banking corporation. As a result, it was not done in this way for all banks. In practice, whenever the ATMs needed a system update, it was done by a remote server that updated all the machines at once. So in other words, this so called "closed system" was not really closed at all, although heavily encrypted. It nevertheless still had some holes for the hackers to get through.⁶⁶ In this case, this is exactly what happened when this Russian syndicate found a hole in the First Commercial Bank's email system and used this hole as a jumping board to get a hold onto to their ATM system, making all of their ATM machines into mechanical zombies.

After the investigations by police and MJIB, all suspects were held in custody and went through subsequent legal proceedings. Taiwanese authority were lucky to crack this case on time, serving as a strong warning for other criminal syndicates who were considering taking Taiwan's financial institutions for their future illegal activities. As for the First Commercial Bank, they decided to scrutinize their firewall and internet security system to prevent their email systems from being further attacked by phishing emails. Even though First Commercial Bank had recovered most of the lost cash, this incident had exposed the bank's two important weak points: outdated hardware and weak internet security system. These two points served to be the perfect opportunity for the Russian syndicate to take advantage of, to perform this magical case. As a result, after the investigation was mostly completed, the chairman of First Commercial Bank, Mr. Tsai had resigned accordingly.

66. *Ibid.*

X. AN INTERVIEW WITH AN INSIDER

On October 1, 2016, the author had an interview with an officer from the First Commercial Bank IT department. As he requested to remain anonymous, he will be referred to as "Mr. Wang" in this paper. According to Mr. Wang, regardless of any kind of ATM, the ATM consisted of two levels to complete operation. The upper level is known as the "Application Level" (AP) and the lower level is known as the "Firmware," which is the one controlling the operating system such as Windows. Most of the encryption, anti-virus software, and guarding system are usually limited at the AP level. On the firmware level, usually regarded as the internal level, its security risk level is relatively low. Thus, the guarding arrangements are usually not as strong as the AP level. If we use other ways to describe this situation, it can be seen as a house. We usually put a lot of security efforts on our front gate and surrounding walls because they are the area directly in contact with outsiders but we usually do not put a lot of security arrangements in the interior of the house. People usually will not put CCTV's inside the house or create obstacles and lock up every room in the house all the time. The reason for this is that we usually think that once the external part is safe, then the interior of the house should be safe, as well. Now if there is thief that can create some way that can instruct someone or somehow to open the front gate for them to enter your house effortlessly, then even if you had the Chinese Great Wall surrounding your house, it would still be useless against those thieves. The situation in the First Commercial Bank was exactly the same.

After First Commercial Bank had done a comprehensive investigation internally, they had concluded few main reasons that made this case possible. First of all, the ATM machine was out of date, which was why they later changed all the Wincor Pro Cash 1500 models to a newer one. Secondly, accordingly to Mr. Wang, the leader of their IT department was not exactly a professional—the person was merely a transfer from other departments based on normal promotion procedure. Thus, they had a scenario where the unprofessional was leading the professional. As a result, the IT department in the First Commercial Bank could not look to the whole cyber security in a broader prospective. Instead, they concentrated on the day-to-day operations of the system that mainly focused on the AP level. Third, and most importantly, as this point had never been disclosed to the public, after thorough internal investigation, besides the malware found on the ATMs by the MJIB as discussed earlier, they also found Trojan EXEs among their high level executive staff. In other words, due to the lack of cyber safety awareness, their high level executive staff may have been the ones responsible for the thief's attack. According to Mr. Wang, the same day the three suspects were officially charged by the Taiwanese

prosecutor, there was another major attack from Russia at the First Commercial Bank's firmware level, though this was never disclosed to the public. This means, our earlier discussion on the malware infiltrating the system via First Commercial Bank's London branch or malware that self-destruct, may only have been a part of the problem. In theory, if that was the only problem, once it was determined by the MJIB, the foreign end should not have possessed the ability to attack First Commercial Bank again. But that had been done on September 13, 2016, the day where Andrejs and other two were charged with fraud (詐欺) and disruption of computer usage (妨害電腦使用), whereby Taiwanese prosecutors demanded 12 years sentences.⁶⁷

According to Mr. Wang, the problem of the attack on the First Commercial Bank on September 13, 2016 had never been fully determined by both MJIB and their own internal IT department. That attack had been seen as a kind of demonstration by the Russian syndicate by the authority and their bank. In short, based on Mr. Wang's statement, the real problem of the First Commercial Bank heist had never been fully identified by both the authority and their bank. The story prescribed earlier in this paper was only the story that the authority and the First Commercial Bank released to the public to avoid public panic and maintain their commercial reputation. There is still a possibility that this or a similar case may still happen to First Commercial Bank or other Taiwan financial institutions in the future.

A. Recommendation from the First Commercial Bank Heist

After the First Commercial Bank's heist, more similar cases occurred around the globe. The latest one was in Thailand. As we can accurately and truly identify the cause of these kinds of activities, it is foreseeable that these kind of cases will continue to be happen around the world. Some expert suggest that the cyber world cop and thieves is like an old Chinese saying "while the priest climbs a foot, the devil climbs ten" (道高一尺魔高一丈). So cyber thieves will always find some new ways to get around the system. Nevertheless, as a tentative conclusion for the First Commercial Bank's heist, a few recommendations may be put into practice to create more "difficulties" in the information technology (IT) environment for those cyber thieves, to minimize the risk of similar incidents from happening again.

67. On 25th January, 2017, Andrejs and others were sentenced to 5 years and a penalty of TWD 600,000 (19,014 USD), will also be evicted once the sentenced served. Jiao Jia Hui "The three suspects of the First Commercial Bank case sentenced to 5 years each, and will be evicted once sentence served <http://www.storm.mg/article/216936>. 2017-01-25.

1. The ATMs machine hardware must be updated to the latest model. If that is not economically possible, then the software operating system of the machine must be kept updated.
2. The cyber security system must be designed towards both the AP level and firmware level. In addition, there must also be a cyber-security system also guarding the internal system of the Bank.
3. There should be a "white list" (白名單) with all the safe software operating in the system and only the software from the white list could be used and operated. Once any foreign software not within that white list are identified, the alarm bell must be immediately activated to determine whether there is any security breach.
4. The leader of the IT department must be promoted with an IT background. It must not let lay personnel lead IT engineers. Also, more resources must be put into the IT department and personnel education. In fact, the leader of the IT department should be from the board of director's level of executives with an IT background.
5. Different banks must work together for the same objective of achieving a safer cyber banking system.

XI. CONCLUSION

The different kind of cyber wrongs discussed in this article are only a few of the more obvious kinds of cyber wrongs that have occurred in recent years. It is nowhere near an exclusive list for all kinds of cyber wrongs. The cyber world is similar to the real human world, in which all the possible wrong kinds of practice would only be limited by your imagination. This is the reason we closely looked into the Taiwanese case of the First Commercial Bank's heist. The author always likes to use the old Chinese saying, "the priest climbs a foot the devils climbs ten." In the cyber world, it is exactly like this: the authority climbs a foot, the criminals climb ten. Based on the analysis of the First Commercial Bank's heist, both the bank and the Taiwanese authority could not 100% identify and prevent the problem. Thus, it can be an inference that a lot of Taiwanese banks or banks around the world are almost like sitting ducks waiting for cyber criminals to shoot.

Looking back at Mainland China, it is a fact that China has the toughest legal arrangements on internet wrongs. Many even suggest China's tough implementation of various internet usage regulations actually kills

people's creativity and affects people's freedom of speech, which is a constitutional right under the Chinese Constitution.⁶⁸ In addition to this, although the Chinese government never admits that there exists this so called "The Chinese Great Firewall," its existence is generally a public knowledge. With this great firewall, one cannot freely peruse many international websites, such as Facebook, overseas news agencies, and sites deemed improper by the Chinese government. Accordingly, in theory the Chinese government should have an upper hand in war against cyber wrongs. However, just like the famous slogan in Jurassic Park, "*Life will find its own course.*" If we admit human minds are limitless, then we must also admit that new forms of cyber wrongs, both crime and tort, will without any doubt appear endlessly in the near future.

Finally, although a lot of these forms of cyber wrongs are clearly illegal such as cyber theft, hacking, destroying cyber properties, or overtaking other people's net accounts, a lot of these cyber wrongs may not be totally illegal but depend on the judgment and value of a particular society. For example, cyber hyper could be a form of advertising tactics and cyber pornography, cybersex, or cyber gambling could purely be a matter of the value judgment of the society. If the Chinese society and government legalized pornography (like in the United States with limitation) and prostitution (like Australia in certain states) and gambling (like Australia with limitation), then the problem of cyber pornography, cyber-sex, and cyber gambling would immediately become no problem at all. Thus, the resources originally used against these kinds of cyber wrongs could be put into areas to battle against the real and more serious type of cyber-criminal activities, such as the First Commercial Bank heist.

68. The Constitution of the People's Republic of China, Article 35.

*Maryland Series
in Contemporary Asian Studies*

(Formerly Occasional Papers/Reprints Series
in Contemporary Asian Studies, 1977-1999)

500 West Baltimore Street
Baltimore, Maryland 21201-1786
U.S.A.

Tel: (410) 706-3870

Fax: (410) 706-1516

(For back issues, new prices effective from October 1, 1991)

1977 Series

- | | | |
|---|-----------------------|---------------------------|
| No. 1 - 1977 | ISSN 0730-0107 | ISBN 0-942182-00-6 |
| Chinese Attitude Toward Continental Shelf and Its Implication on De-
limiting Seabed in Southeast Asia (Hungdah CHIU), 32 pp. \$3.00 | | |
| No. 2 - 1977 | ISSN 0730-0107 | ISBN 0-942182-01-4 |
| Income Distribution in the Process of Economic Growth of the Repub-
lic of China (Yuan-Li WU), 45 pp. \$3.00 | | |
| No. 3 - 1977 | ISSN 0730-0107 | ISBN 0-942182-02-2 |
| The Indonesian Maoists: Doctrines and Perspectives (Justus M. van der
Kroef), 31 pp. \$3.00 | | |
| No. 4 - 1977 | ISSN 0730-0107 | ISBN 0-942182-03-0 |
| Taiwan's Foreign Policy in the 1970s: A Case Study Adaptation and
Viability (Thomas J. Bellows), 22 pp. \$3.00 | | |
| No. 5 - 1977 | ISSN 0730-0107 | ISBN 0-942182-04-9 |
| Asian Political Scientists in North America: Professional and Ethnic
Problems (Edited by Chun-tu HSUEH), 148 pp. Index \$6.00 | | |
| No. 6 - 1977 | ISSN 0730-0107 | ISBN 0-942182-05-7 |
| The Sino-Japanese Fisheries Agreement of 1975: A Comparison with
Other North Pacific Fisheries Agreements (SONG Yook Hong), 80
pp. \$5.00 | | |

- No. 7 - 1977** **ISSN 0730-0107** **ISBN 0-942182-06-5**
 Foreign Trade Contracts Between West German Companies and the
 People's Republic of China: A Case Study (Robert Heuser), 22 pp.
 \$3.00
- No. 8 - 1977** **ISSN 0730-0107** **ISBN 0-942182-07-3**
 Reflections on Crime and Punishment in China, with Appended Sen-
 tencing Documents (Randle Edwards, Translation of Documents
 by Randle Edwards and Hungdah CHIU), 67 pp. \$3.00
- No. 9 - 1977** **ISSN 0730-0107** **ISBN 0-942182-08-1**
 Chinese Arts and Literature: A Survey of Recent Trends (Edited by
 Wai-lim YIP), 126 pp. \$5.00
- No. 10 - 1977** **ISSN 0730-0107** **ISBN 0-942182-09-X**
 Legal Aspects of U.S.-Republic of China Trade and Investment -- Pro-
 ceedings of a Regional Conference of the American Society of In-
 ternational Law (Edited by Hungdah CHIU and David Simon),
 217 pp. Index \$8.00
- No. 11 - 1977** **ISSN 0730-0107** **ISBN 0-942182-10-3**
 Asian American Assembly Position Paper: I. A Review of U.S. China
 Relations, 62 pp. \$3.00
- No. 12 - 1977** **ISSN 0730-0107** **ISBN 0-942182-11-1**
 Asian American Assembly Position Paper: II. A Review of U.S. Em-
 ployment Policy, 24 pp. \$3.00

1978 Series

- No. 1 - 1978 (13)** **ISSN 0730-0107** **ISBN 0-942182-12-X**
 Indian Ocean Politics: An Asian-African Perspective (K.P. Misra), 31
 pp. \$3.00
- No. 2 - 1978 (14)** **ISSN 0730-0107** **ISBN 0-942182-13-8**
 Normalizing Relations with the People's Republic of China: Problems,
 Analysis, and Documents (Edited by Hungdah CHIU, with contri-
 bution by G. J. Sigur, Robert A. Scalapino, King C. Chen, Eugene
 A. Theroux, Michael Y.M. Kau, James C. Hsiung and James W.
 Morley), 207 pp. Index \$5.00
- No. 3 - 1978 (15)** **ISSN 0730-0107** **ISBN 0-942182-14-6**
 Growth, Distribution, and Social Change: Essays on the Economy of
 the Republic of China (Edited by Yuan-li WU and Kung-chia
 YEH), 227 pp. Index \$5.00
- No. 4 - 1978 (16)** **ISSN 0730-0107** **ISBN 0-942182-15-4**
 The Societal Objectives of Wealth, Growth, Stability, and Equity in Tai-
 wan (Jan S. Prybyla), 31 pp. \$3.00

- No. 5 - 1978 (17)** **ISSN 0730-0107** **ISBN 0-942182-16-2**
The Role of Law in the People's Republic of China as Reflecting Mao
Tse-Tung's Influence (Shao-chuan LENG), 18 pp. \$3.00
- No. 6 - 1978 (18)** **ISSN 0730-0107** **ISBN 0-942182-17-0**
Criminal Punishment in Mainland China: A Study of Some Yunnan
Province Documents (Hungdah CHIU), 35 pp. \$3.00
- No. 7 - 1978 (19)** **ISSN 0730-0107** **ISBN 0-942182-18-9**
A Guide to the Study of Japanese Law (Lawrence W. Beer and Hide-
nori Tomatsu), 45 pp. \$4.00
- No. 8 - 1978 (20)** **ISSN 0730-0107** **ISBN 0-942182-19-7**
The Pueblo, EC-121, and Mayaguez Incidents: Some Continuities and
Changes (Robert Simmons), 40 pp. \$4.00
- No. 9 - 1978 (21)** **ISSN 0730-0107** **ISBN 0-942182-20-0**
Two Korea's Unification Policy and Strategy (Yong Soon YIM), 82 pp.
Index \$4.00

1979 Series

- No. 1 - 1979 (22)** **ISSN 0730-0107** **ISBN 0-942182-21-9**
Asian Immigrants and Their Status in the U.S. (Edited by Hungdah
CHIU), 54 pp. \$4.00
- No. 2 - 1979 (23)** **ISSN 0730-0107** **ISBN 0-942182-22-7**
Social Disorder in Peking After the 1976 Earthquake Revealed by a
Chinese Legal Documents (Hungdah CHIU), 20 pp. \$4.00
- No. 3 - 1979 (24)** **ISSN 0730-0107** **ISBN 0-942182-23-5**
The Dragon and the Eagle — A Study of U.S.-People's Republic of
China Relations in Civil Air Transport (Jack C. Young), 65 pp. \$5.00
- No. 4 - 1979 (25)** **ISSN 0730-0107** **ISBN 0-942182-24-3**
Chinese Women Writers Today (Edited by Wai-lim YIP and William
Tay), 108 pp. \$5.00
- No. 5 - 1979 (26)** **ISSN 0730-0107** **ISBN 0-942182-25-1**
Certain Legal Aspects of Recognizing the People's Republic of China
(Hungdah CHIU), 49 pp. \$4.00
- No. 6 - 1979 (27)** **ISSN 0730-0107** **ISBN 0-942182-26-X**
China's Nationalization of Foreign Firms: The Politics of Hostage Cap-
italism, 1949-1957 (Thomas N. Thompson), 80 pp. Index \$5.00

- No. 7 - 1979 (28)** **ISSN 0730-0107** **ISBN 0-942182-27-8**
 U.S. Status of Force Agreement with Asian Countries: Selected Studies
 (Charles Cochran and Hungdah CHIU), 130 pp. Index \$4.00
- No. 8 - 1979 (29)** **ISSN 0730-0107** **ISBN 0-942182-28-6**
 China's Foreign Aid in 1978 (John F. Copper), 45 pp. \$4.00

1980 Series

- No. 1 - 1980 (30)** **ISSN 0730-0107** **ISBN 0-942182-29-4**
 The Chinese Connection and Normalization (Edited by Hungdah
 CHIU and Karen Murphy), 200 pp. Index \$7.00
- No. 2 - 1980 (31)** **ISSN 0730-0107** **ISBN 0-942182-30-8**
 The Conceptual Foundations of U.S. China Policy: A Critical Review
 (James C. Hsiung), 17 pp. \$3.00
- No. 3 - 1980 (32)** **ISSN 0730-0107** **ISBN 0-942182-31-6**
 Policy, Proliferation and the Nuclear Proliferation Treaty: U.S. Strate-
 gies and South Asian Prospects (Joanne Finegan), 61 pp. \$4.00
- No. 4 - 1980 (33)** **ISSN 0730-0107** **ISBN 0-942182-32-4**
 A Comparative Study of Judicial Review Under Nationalist Chinese
 and American Constitutional Law (Jyh-pin FA), 200 pp. Index \$6.00
- No. 5 - 1980 (34)** **ISSN 0730-0107** **ISBN 0-942182-33-2**
 Certain Problems in Recent Law Reform in the People's Republic of
 China (Hungdah CHIU), 34 pp. \$4.00
- No. 6 - 1980 (35)** **ISSN 0730-0107** **ISBN 0-942182-34-0**
 China's New Criminal & Criminal Procedure Codes (Hungdah CHIU),
 16 pp. \$3.00
- No. 7 - 1980 (36)** **ISSN 0730-0107** **ISBN 0-942182-35-9**
 China's Foreign Relations: Selected Studies (Edited by F. Gilbert Chan
 & Ka-che YIP), 115 pp. \$5.00
- No. 8 - 1980 (37)** **ISSN 0730-0107** **ISBN 0-942182-36-7**
 Annual Review of Selected Books on Contemporary Asian Studies
 (1979-1980) (Edited by John F. Copper), 45 pp. \$4.00

1981 Series

- No. 1 - 1981 (38)** **ISSN 0730-0107** **ISBN 0-942182-37-5**
 Structural Changes in the Organization and Operation of China's Crim-
 inal Justice System (Hungdah CHIU), 31 pp. \$3.00

- No. 2 - 1981 (39)** **ISSN 0730-0107** **ISBN 0-942182-38-3**
Readjustment and Reform in the Chinese Economy (Jan S. Prybyla), 58 pp. \$3.00
- No. 3 - 1981 (40)** **ISSN 0730-0107** **ISBN 0-942182-39-1**
Symposium on the Trial of Gang of Four and Its Implication in China (Edited by James C. Hsiung), 118 pp. \$5.00
- No. 4 - 1981 (41)** **ISSN 0730-0107** **ISBN 0-942182-40-5**
China and the Law of the Sea Conference (Hungdah CHIU), 30 pp. \$4.00
- No. 5 - 1981 (42)** **ISSN 0730-0107** **ISBN 0-942182-41-3**
China's Foreign Aid in 1979-80 (John Franklin Copper), 54 pp. \$4.00
- No. 6 - 1981 (43)** **ISSN 0730-0107** **ISBN 0-942182-42-1**
Chinese Regionalism: Yesterday and Today (Franz Michael), 35 pp. \$4.00
- No. 7 - 1981 (44)** **ISSN 0730-0107** **ISBN 0-942182-43-X**
Elite Conflict in the Post-Mao China (Parris H. Chang), 40 pp. \$4.00
(Please order No. 2 - 1983 (55) for a revised version of this issue.)
- No. 8 - 1981 (45)** **ISSN 0730-0107** **ISBN 0-942182-44-8**
Proceedings of Conference on Multi-system Nations and International Law: International Status of Germany, Korea, and China (Edited by Hungdah CHIU and Robert Downen), 203 pp. Index \$8.00

1982 Series

- No. 1 - 1982 (46)** **ISSN 0730-0107** **ISBN 0-942182-45-6**
Socialist Legalism: Reform and Continuity in Post-Mao People's Republic of China (Hungdah CHIU), 35 pp. \$4.00
- No. 2 - 1982 (47)** **ISSN 0730-0107** **ISBN 0-942182-46-4**
Kampuchea: The Endless Tug of War (Justus M. Van der Kroef), 51 pp. \$4.00
- No. 3 - 1982 (48)** **ISSN 0730-0107** **ISBN 0-942182-47-2**
Social Change on Mainland China and Taiwan, 1949-1980 (Alan P.L. Liu), 55 pp. \$5.00
- No. 4 - 1982 (49)** **ISSN 0730-0107** **ISBN 0-942182-48-0**
Taiwan's Security and United States Policy: Executive and Congressional Strategies in 1978-1979 (Michael S. Frost), 39 pp. \$4.00

- No. 5 - 1982 (50)** **ISSN 0730-0107** **ISBN 0-942182-49-9**
 Constitutional Revolution in Japanese Law, Society and Politics
 (Lawrence W. Beer), 35 pp. \$4.00
- No. 6 - 1982 (51)** **ISSN 0730-0107** **ISBN 0-942182-50-2**
 Review of Selected Books on Contemporary Asian Studies, 1981-1982
 (Edited by David Salem, Roy Werner and Lyushen Shen), 67 pp. \$4.00
- No. 7 - 1982 (52)** **ISSN 0730-0107** **ISBN 0-942182-51-0**
 Chinese Law and Justice: Trends Over Three Decades (Hungdah
 CHIU), 39 pp. \$4.00
- No. 8 - 1982 (53)** **ISSN 0730-0107** **ISBN 0-942182-52-9**
 Disarmament and Civilian Control in Japan: A Constitutional Dilemma
 (Theodore McNelly), 16 pp. \$4.00

1983 Series

- No. 1 - 1983 (54)** **ISSN 0730-0107** **ISBN 0-942182-53-7**
 Essays on Sun Yat-sen and the Economic Development of Taiwan (Ma-
 ria Hsia Chang and A. James Gregor), 60 pp. \$3.00
- No. 2 - 1983 (55)** **ISSN 0730-0107** **ISBN 0-942182-54-5**
 Elite Conflict in the Post-Mao China (Revised version of No. 7-1981
 (44)) (Parris H. Chang), 48 pp. \$3.00
- No. 3 - 1983 (56)** **ISSN 0730-0107** **ISBN 0-942182-55-3**
 Media-Coverage on Taiwan in The People's Republic of China (Jörg-M.
 Rudolph), 77 pp. \$4.00
- No. 4 - 1983 (57)** **ISSN 0730-0107** **ISBN 0-942182-56-1**
 Transit Problems of Three Asian Land-locked Countries: Afghanistan,
 Nepal and Laos (Martin Ira Glassner), 55 pp. \$3.00
- No. 5 - 1983 (58)** **ISSN 0730-0107** **ISBN 0-942182-57-X**
 China's War Against Vietnam: A Military Analysis (King C. Chen),
 33 pp. \$3.00
- No. 6 - 1983 (59)** **ISSN 0730-0107** **ISBN 0-942182-58-8**
 The People's Republic of China, International Law and Arms Control
 (David Salem), 325 pp. Index \$7.00
 (Hardcover edition published in *Maryland Studies in East Asian Law and
 Politics Series*, No. 3, ISBN 0-942182-59-6) \$15.00

1984 Series

- No. 1 - 1984 (60)** **ISSN 0730-0107** **ISBN 0-942182-60-X**
 China's Nuclear Policy: An Overall View (Shao-chuan LENG), 18 pp. \$3.00
- No. 2 - 1984 (61)** **ISSN 0730-0107** **ISBN 0-942182-61-8**
 The Communist Party of China: Party Powers and Group Politics from the Third Plenum to the Twelfth Party Congress (Hung-mao TIEN), 30 pp. \$3.00
- No. 3 - 1984 (62)** **ISSN 0730-0107** **ISBN 0-942182-62-6**
 Legal Problems of Seabed Boundary Delimitation in the East China Sea (Ying-jeou MA), 308 pp. Index (out of print) \$10.00
 (Hardcover edition published in *Maryland Studies in East Asian Law and Politics Series*, No. 4, ISBN 0-942182-63-4) \$15.00
- No. 4 - 1984 (63)** **ISSN 0730-0107** **ISBN 0-942182-64-2**
 A New Direction in Japanese Defense Policy: Views from the Liberal Democratic Party Diet Members (Steven Kent Vogel), 63 pp. \$3.00
- No. 5 - 1984 (64)** **ISSN 0730-0107** **ISBN 0-942182-65-0**
 Taiwan's Elections: Political Development and Democratization in the Republic of China (John F. Copper with George P. Chen), 180 pp. Index \$5.00
 (Hardcover edition: ISBN 0-942182-66-9) \$10.00
- No. 6 - 1984 (65)** **ISSN 0730-0107** **ISBN 0-942182-67-7**
 Cankao Xiaoxi: Foreign News in the Propaganda System of the People's Republic of China (Jörg-Meinhard Rudolph), 174 pp. Index \$5.00

1985 Series

- No. 1 - 1985 (66)** **ISSN 0730-0107** **ISBN 0-942182-68-5**
 The Political Basis of the Economic and Social Development in the Republic of China (Alan P. L. Liu), 22 pp. \$3.00
- No. 2 - 1985 (67)** **ISSN 0730-0107** **ISBN 0-942182-69-3**
 The Legal System and Criminal Responsibility of Intellectuals in the People's Republic of China, 1949-1982 (Carlos Wing-hung Lo), 125 pp. Index \$5.00
- No. 3 - 1985 (68)** **ISSN 0730-0107** **ISBN 0-942182-70-7**
 Symposium on Hong Kong: 1997 (Edited by Hungdah CHIU), 100 pp. Index \$4.00

- No. 4 - 1985 (69)** **ISSN 0730-0107** **ISBN 0-942182-71-5**
The 1982 Chinese Constitution and the Rule of Law (Hungdah CHIU),
18 pp. (out of print) \$3.00
- No. 5 - 1985 (70)** **ISSN 0730-0107** **ISBN 0-942182-72-3**
Peking's Negotiating Style: A Case study of U.S.-PRC Normalization
(Jaw-Ling Joanne CHANG), 22 pp. \$3.00
- No. 6 - 1985 (71)** **ISSN 0730-0107** **ISBN 0-942182-73-1**
China's Marine Environmental Protection Law: The Dragon Creeping
in Murky Waters (Mitchell A. Silk), 32 pp. \$3.00

1986 Series

- No. 1 - 1986 (72)** **ISSN 0730-0107** **ISBN 0-942182-74-X**
From Tradition to Modernity: A Socio-Historical Interpretation on
China's Struggle toward Modernization Since the Mid-19th Cen-
tury (Wen-hui TSAI), 76 pp. \$4.00
- No. 2 - 1986 (73)** **ISSN 0730-0107** **ISBN 0-942182-75-8**
Peace and Unification in Korea and International Law (Byung-Hwa
LYOU), 205 pp. Index. \$8.00
- No. 3 - 1986 (74)** **ISSN 0730-0107** **ISBN 0-942182-76-6**
The Hong Kong Agreement and American Foreign Policy (Hungdah
CHIU), 18 pp. \$3.00
- No. 4 - 1986 (75)** **ISSN 0730-0107** **ISBN 0-942182-77-4**
United States-China Normalization: An Evaluation of Foreign Policy
Decision Making (Jaw-ling Joanne CHANG), copublished with
Monograph Series in World Affairs, University of Denver, 246 pp.
Index. (out of print) \$8.00
(Hardcover edition published in Maryland Studies in East Asian Law and Politics
Series, No. 7. ISBN 0-942182-78-2) \$12.00
- No. 5 - 1986 (76)** **ISSN 0730-0107** **ISBN 0-942182-79-0**
Communications and China's National Integration: An Analysis of
People's Daily and *Central Daily* on the China Reunification Issue
(Shuhua CHANG), 205 pp. \$8.00
- No. 6 - 1986 (77)** **ISSN 0730-0107** **ISBN 0-942182-80-4**
Since Aquino: The Philippine Tangle and the United States (Justus M.
van der Kroef), 73 pp. \$3.00

1987 Series

- No. 1 - 1987 (78)** **ISSN 0730-0107** **ISBN 0-942182-81-2**
An Analysis of the U.S.-China Nuclear Energy Cooperation Agreement
(Benjamin Chin), 40 pp. \$3.00
- No. 2 - 1987 (79)** **ISSN 0730-0107** **ISBN 0-942182-82-0**
Survey of Recent Developments in China (Mainland and Taiwan), 1985-
1986 (edited by Hungdah CHIU, with the assistance of Jaw-ling Jo-
anne CHANG), 222 pp. Index \$8.00
- No. 3 - 1987 (80)** **ISSN 0730-0107** **ISBN 0-942182-83-9**
Democratizing Transition in Taiwan (Yangsun CHOU and Andrew J.
Nathan), 24 pp. \$3.00
- No. 4 - 1987 (81)** **ISSN 0730-0107** **ISBN 0-942182-84-7**
The Legal Status of the Chinese Communist Party (Robert Heuser),
25 pp. \$3.00
- No. 5 - 1987 (82)** **ISSN 0730-0107** **ISBN 0-942182-85-5**
The Joint Venture and Related Contract Laws of Mainland China and
Taiwan: A Comparative Analysis (Clyde D. Stoltenberg and David
W. McClure), 54 pp. \$4.00
- No. 6 - 1987 (83)** **ISSN 0730-0107** **ISBN 0-942182-86-3**
Reform in Reverse: Human Rights in the People's Republic of China,
1986/1987 (Ta-Ling LEE and John F. Copper), 150 pp. \$8.00

1988 Series

- No. 1 - 1988 (84)** **ISSN 0730-0107** **ISBN 0-942182-87-1**
Chinese Attitudes toward International Law in the Post-Mao Era, 1978-
1987 (Hungdah CHIU), 41 pp. \$3.00
- No. 2 - 1988 (85)** **ISSN 0730-0107** **ISBN 0-942182-88-X**
Chinese Views on the Sources of International Law (Hungdah CHIU),
20 pp. \$3.00
- No. 3 - 1988 (86)** **ISSN 0730-0107** **ISBN 0-942182-89-8**
People's Republic of China: The Human Rights Exception (Roberta
Cohen), 103 pp. (out of print) \$5.00
- No. 4 - 1988 (87)** **ISSN 0730-0107** **ISBN 0-942182-90-1**
Settlement of the Macau Issue: Distinctive Features of Beijing's Negoti-
ating Behavior (with text of 1887 Protocol and 1987 Declaration)
(Jaw-ling Joanne CHANG), 37 pp. \$3.00

No. 5 - 1988 (88) **ISSN 0730-0107** **ISBN 0-942182-91-X**
 The Draft Basic Law of Hong Kong: Analysis and Documents (edited
 by Hungdah CHIU), 153 pp. \$5.00

No. 6 - 1988 (89) **ISSN 0730-0107** **ISBN 0-942182-92-8**
 Constitutionalism in Asia: Asian Views of the American Influence
 (edited by Lawrence W. Beer), 210 pp. \$10.00

1989 Series

No. 1 - 1989 (90) **ISSN 0730-0107** **ISBN 0-925153-00-1**
 The Right to a Criminal Appeal in the People's Republic of China
 (Margaret Y.K. Woo), 43 pp. \$3.00

No. 2 - 1989 (91) **ISSN 0730-0107** **ISBN 0-925153-01-X**
 The Status of Customary International Law, Treaties, Agreements and
 Semi-Official or Unofficial Agreements in Chinese Law (Hungdah
 CHIU), 22 pp. \$3.00

No. 3 - 1989 (92) **ISSN 0730-0107** **ISBN 0-925153-02-8**
 One Step Forward, One Step Back, Human Rights in the People's Re-
 public of China in 1987/88 (John F. Cooper and Ta-ling LEE), 140
 pp. \$6.00

No. 4 - 1989 (93) **ISSN 0730-0107** **ISBN 0-925153-03-6**
 Tibet: Past and Present (Hungdah CHIU and June Teufel Dreyer), 25
 pp. \$3.00

No. 5 - 1989 (94) **ISSN 0730-0107** **ISBN 0-925153-04-4**
 Chinese Attitude toward International Law of Human Rights in the
 Post-Mao Era (Hungdah CHIU), 38 pp. \$4.00

No. 6 - 1989 (95) **ISSN 0730-0107** **ISBN 0-925153-05-2**
 Tibet to Tiananmen: Chinese Human Rights and United States Foreign
 Policy (W. Gary Vause), 47 pp. \$4.00

1990 Series

No. 1 - 1990 (96) **ISSN 0730-0107** **ISBN 0-925153-06-0**
 The International Legal Status of the Republic of China (Hungdah
 CHIU), 20 pp. (Please order No. 5-1992 (112) for a revised version
 of this issue) \$3.00

No. 2 - 1990 (97) **ISSN 0730-0107** **ISBN 0-925153-07-9**
 Tiananmen: China's Struggle for Democracy—Its Prelude, Development, Aftermath, and Impact (Winston L. Y. Yang and Marsha L. Wagner), 314 pp. Index (paperback out of print) \$8.00
 (Hardcover edition published in *Maryland Studies in East Asian Law and Politics Series*, No. 11, ISBN 0-925153-08-7) \$14.00

No. 3 - 1990 (98) **ISSN 0730-0107** **ISBN 0-925153-09-5**
 Nationality and International Law in Chinese Perspective (Hungdah CHIU), 37 pp. \$4.00

No. 4 - 1990 (99) **ISSN 0730-0107** **ISBN 0-925153-10-9**
 The Taiwan Relations Act after Ten Years (Lori Fisler Damrosch), 27 pp. \$3.00

No. 5 - 1990 (100) **ISSN 0730-0107** **ISBN 0-925153-11-7**
 The Taiwan Relations Act and Sino-American Relations (Hungdah CHIU), 34 pp. (out of print) \$4.00

No. 6 - 1990 (101) **ISSN 0730-0107** **ISBN 0-925153-12-5**
 Taiwan's Recent Elections: Fulfilling the Democratic Promise (John F. Copper), 174 pp. Index (out of print) \$8.00

1991 Series

No. 1 - 1991 (102) **ISSN 0730-0107** **ISBN 0-925153-13-3**
 Legal Aspects of Investment and Trade with the Republic of China (Edited by John T. McDermott, with contributions by Linda F. Powers, Ronald A. Case, Chung-Teh LEE, Jeffrey H. Chen, Cheryl M. Friedman, Hungdah CHIU, K.C. Fan and Douglas T. Hung), 94 pp. \$6.00

No. 2 - 1991 (103) **ISSN 0730-0107** **ISBN 0-925153-14-1**
 Failure of Democracy Movement: Human Rights in the People's Republic of China, 1988/89 (Ta-ling LEE and John F. Copper), 150 pp. Index \$10.00

No. 3 - 1991 (104) **ISSN 0730-0107** **ISBN 0-925153-15-X**
 Freedom of Expression: The Continuing Revolution in Japan's Legal Culture (Lawrence W. Beer), 31 pp. \$5.00

No. 4 - 1991 (105) **ISSN 0730-0107** **ISBN 0-925153-16-8**
 The 1989 US-Republic of China (Taiwan) Fisheries Negotiations (Mark Mon-Chang Hsieh), 84 pp. \$6.00

No. 5 - 1991 (106) **ISSN 0730-0107** **ISBN 0-925153-17-6**
 Politics of Divided Nations: China, Korea, Germany and Vietnam — Unification, Conflict Resolution and Political Development (Edited by Quansheng ZHAO and Robert Sutter), 198 pp. Index \$12.00

No. 6 - 1991 (107)

ISSN 0730-0107

ISBN 0-925153-18-4

Lawyers in China: The Past Decade and Beyond (Timothy A. Gelatt),
49 pp.

\$5.00

1992 Series

No. 1 - 1992 (108)

ISSN 0730-0107

ISBN 0-925153-19-2

Judicial Review of Administration in the People's Republic of China
(Jyh-pin FA & Shao-chuan LENG), 37 pp.

\$5.00

No. 2 - 1992 (109)

ISSN 0730-0107

ISBN 0-925153-20-6

China's Ministry of State Security: Coming of Age in the International
Arena (Nicholas Eftimiades), 24 pp.

\$4.00

No. 3 - 1992 (110)

ISSN 0730-0107

ISBN 0-925153-21-4

Libel Law and the Press in South Korea: An Update (KYU Ho Youm),
23 pp.

\$5.00

No. 4 - 1992 (111)

ISSN 0730-0107

ISBN 0-925153-22-2

Tiananmen Aftermath: Human Rights in the People's Republic of
China, 1990 (John F. Copper and Ta-ling LEE), 133 pp. Index

\$15.00

No. 5 - 1992 (112)

ISSN 0730-0107

ISBN 0-925153-23-0

The International Legal Status of the Republic of China (Revised ver-
sion of No. 1-1990 (96)) (Hungdah CHIU), 37 pp.

\$4.00

No. 6 - 1992 (113)

ISSN 0730-0107

ISBN 0-925153-24-9

China's Criminal Justice System and the Trial of Pro-Democracy Dissi-
dents (Hungdah CHIU), 21 pp.

\$3.00

1993 Series

No. 1 - 1993 (114)

ISSN 0730-0107

ISBN 0-925153-25-7

Can One Unscramble an Omelet? China's Economic Reform in Theory
and Practice (Yuan-li WU and Richard Y. C. Yin), 34 pp.

\$4.00

No. 2 - 1993 (115)

ISSN 0730-0107

ISBN 0-925153-26-5

Constitutional Development and Reform in the Republic of China on
Taiwan (With Documents) (Hungdah CHIU), 61 pp.

\$6.00

No. 3 - 1993 (116)

ISSN 0730-0107

ISBN 0-925153-27-3

Sheltering for Examination (*Shourong Shencha*) in the Legal System of
the People's Republic of China (Tao-tai HSIA and Wendy I.
Zeldin), 32 pp.

\$4.00

No. 4 - 1993 (117) **ISSN 0730-0107** **ISBN 0-925153-28-1**
 In Making China Modernized: Comparative Modernization between
 Mainland China and Taiwan (Wen-hui TSAI), 281 pp. Index (out
 of print, please order No. 5 - 1996 for 2nd ed.) \$18.00

No. 5 - 1993 (118) **ISSN 0730-0107** **ISBN 0-925153-30-3**
 Hong Kong's Transition to 1997: Background, Problems and Prospects
 (with Documents) (Hungdah CHIU), 106 pp. \$7.00

No. 6 - 1993 (119) **ISSN 0730-0107** **ISBN 0-925153-31-1**
 Koo-Wang Talks and the Prospect of Building Constructive and Stable
 Relations Across the Taiwan Straits (with Documents) (Hungdah
 CHIU), 69 pp. \$5.00

1994 Series

No. 1 - 1994 (120) **ISSN 0730-0107** **ISBN 0-925153-32-X**
 Statutory Encouragement of Investment and Economic Development in
 the Republic of China on Taiwan (Neil L. Meyers), 72 pp. \$7.00

No. 2 - 1994 (121) **ISSN 0730-0107** **ISBN 0-925153-33-8**
 Don't Force Us to Lie: The Struggle of Chinese Journalists in the Re-
 form Era (Allison Liu Jernow), 99 pp. \$7.00

No. 3 - 1994 (122) **ISSN 0730-0107** **ISBN 0-925153-34-6**
 Institutionalizing a New Legal System in Deng's China (Hungdah
 CHIU), 44 pp. \$5.00

No. 4 - 1994 (123) **ISSN 0730-0107** **ISBN 0-925153-35-4**
 The Bamboo Gulag: Human Rights in the People's Republic of China,
 1991-1992 (Ta-ling LEE & John F. Copper), 281 pp. Index \$20.00

No. 5 - 1994 (124) **ISSN 0730-0107** **ISBN 0-925153-36-2**
 Taiwan's Legal System and Legal Profession (Hungdah CHIU and
 Jyh-pin FA), 22 pp. \$3.00

No. 6 - 1994 (125) **ISSN 0730-0107** **ISBN 0-925153-37-0**
 Toward Greater Democracy: An Analysis of the Republic of China on
 Taiwan's Major Elections in the 1990s (Wen-hui TSAI), 40 pp. \$6.00

1995 Series

No. 1 - 1995 (126) **ISSN 0730-0107** **ISBN 0-925153-38-9**
 Relations between the Republic of China and the Republic of Chile
 (Herman Gutierrez B. and Lin CHOU), 31 pp. \$5.00

- No. 2 - 1995 (127)** **ISSN 0730-0107** **ISBN 0-925153-39-7**
The Tibet Question and the Hong Kong Experience (Barry Sautman
and Shiu-hing LO), 82 pp. \$10.00
- No. 3 - 1995 (128)** **ISSN 0730-0107** **ISBN 0-925153-40-0**
Mass Rape, Enforced Prostitution, and the Japanese Imperial
Army: Japan Eschews International Legal Responsibility?
(David Boling), 56 pp. \$5.00
- No. 4 - 1995 (129)** **ISSN 0730-0107** **ISBN 0-925153-41-9**
The Role of the Republic of China in the World Economy (Chu-yuan
CHENG), 25 pp. \$3.00
- No. 5 - 1995 (130)** **ISSN 0730-0107** **ISBN 0-925153-42-7**
China's Economy after Deng: A Long-Term Perspective (Peter C.Y.
Chow), 43 pp. \$5.00
- No. 6 - 1995 (131)** **ISSN 0730-0107** **ISBN 0-925153-43-5**
An Entrepreneurial Analysis of Opposition Movements (Ching-chane
HWANG), 179 pp. Index \$18.00

1996 Series

- No. 1 - 1996 (132)** **ISSN 0730-0107** **ISBN 0-925153-44-3**
Taiwan's 1995 Legislative Yuan Election (John F. Copper), 39 pp. \$6.00
- No. 2 - 1996 (133)** **ISSN 0730-0107** **ISBN 0-925153-45-1**
Russian-Taiwanese Relations: Current State, Problems, and Prospects
of Development (Peter M. Ivanov), 76 pp. \$10.00
- No. 3 - 1996 (134)** **ISSN 0730-0107** **ISBN 0-925153-46-X**
Recent Relations between China and Taiwan and Taiwan's Defense Ca-
pabilities (Hungdah CHIU & June Teufel Dreyer), 28 pp. \$4.00
- No. 4 - 1996 (135)** **ISSN 0730-0107** **ISBN 0-925153-47-8**
Intellectual Property Protection in the Asian-Pacific Region: A Com-
parative Study (Paul C. B. Liu & Andy Y. Sun), 183 pp. Index. \$25.00
(Hardcover edition: ISBN 0-925153-48-6) \$32.00
- No. 5 - 1996 (136)** **ISSN 0730-0107** **ISBN 0-925153-49-4**
In Making China Modernized: Comparative Modernization between
Mainland China and Taiwan (2nd ed.) (Wen-hui TSAI), 297 pp.
Index. \$30.00
(Hardcover edition: ISBN 0-925153-50-8) \$37.00

- No. 6 - 1996 (137)** **ISSN 0730-0107** **ISBN 0-925153-51-6**
 A Study of the Consular Convention between the United States of
 America and the People's Republic of China (Stephen Kho), 68 pp. \$6.00

1997 Series

- No. 1 - 1997 (138)** **ISSN 0730-0107** **ISBN 0-925153-52-4**
 Tiananmen to Tiananmen, China under Communism 1947-1996
 (Yuan-Li WU), 348 pp. Index \$35.00
 (Hardcover edition: ISBN 0-925153-53-2) \$45.00
- No. 2 - 1997 (139)** **ISSN 0730-0107** **ISBN 0-925153-54-0**
 The External Relations and International Status of Hong Kong (TING
 Wai), 72 pp. \$8.00
- No. 3 - 1997 (140)** **ISSN 0730-0107** **ISBN 0-925153-55-9**
 Sheltering for Examination (*Shoushen*) in the People's Republic of
 China: Law, Policy, and Practices (Kam C. WONG), 53 pp. \$6.00
- No. 4 - 1997 (141)** **ISSN 0730-0107** **ISBN 0-925153-56-7**
 Legal Aid Practices in the PRC in the 1990s — Dynamics, Contents and
 Implications, (LUO Qizhi) 68 pp. \$8.00
- No. 5 - 1997 (142)** **ISSN 0730-0107** **ISBN 0-925153-57-5**
 The KMT's 15th Party Congress: The Ruling Party at a Crossroads
 (John F. Copper), 38 pp. \$5.00
- No. 6 - 1997 (143)** **ISSN 0730-0107** **ISBN 0-925153-58-3**
 From Pirate King to Jungle King: Transformation of Taiwan's Intellec-
 tual Property Protection (Andy Y. Sun), 138 pp. \$18.00

1998 Series

- No. 1 - 1998 (144)** **ISSN 0730-0107** **ISBN 0-925153-59-1**
 From "Multi-System Nations" to "Linkage Communities": A New
 Conceptual Scheme for the Integration of Divided Nations
 (Yung WEI), 20 pp. \$4.00
- No. 2 - 1998 (145)** **ISSN 0730-0107** **ISBN 0-925153-60-5**
 The Impact of the World Trade Organization on the Lack of Trans-
 parency in the People's Republic of China (Stephen Kho), 63 pp. \$7.00
- No. 3 - 1998 (146)** **ISSN 0730-0107** **ISBN 0-925153-61-3**
 The Nationalist Ideology of the Chinese Military (Xiaoyu CHEN), 45
 pp. \$6.00

No. 4 - 1998 (147) **ISSN 0730-0107** **ISBN 0-925153-62-1**
 Convergence and the Future of Reunification between Mainland China
 and Taiwan: A Developmental View (Wen-hui TSAI), 33 pp. \$5.00

No. 5 - 1998 (148) **ISSN 0730-0107** **ISBN 0-925153-63-X**
 Chinese Patent Law and Patent Litigation in China (Xiang WANG),
 61 pp. \$8.00

No. 6 - 1998 (149) **ISSN 0730-0107** **ISBN 0-925153-64-8**
 The Development of Banking in Taiwan: The Historical Impact on Fu-
 ture Challenges (Lawrence L.C. Lee), 39 pp. \$6.00

1999 Series

No. 1 - 1999 (150) **ISSN 0730-0107** **ISBN 0-925153-65-6**
 An Analysis of the Sino-Japanese Dispute over the T'iaoyutai Islets
 (Senkaku Gunto) (Hungdah CHIU), 27 pp. \$6.00

No. 2 - 1999 (151) **ISSN 0730-0107** **ISBN 0-925153-66-4**
 Taiwan's 1998 Legislative Yuan, Metropolitan Mayoral and City Coun-
 cil Elections: Confirming and Consolidating Democracy in the Re-
 public of China (John F. Copper), 53 pp. \$7.00

No. 3 - 1999 (152) **ISSN 0730-0107** **ISBN 0-925153-67-2**
 The Diaoyutai/Senkaku Islands Dispute: Its History and an Analysis of
 the Ownership Claims of the P.R.C., R.O.C., and Japan
 (Han-yi SHAW), 148 pp. (out of print) \$20.00

No. 4 - 1999 (153) **ISSN 0730-0107** **ISBN 0-925153-68-0**
 Election and Democracy in Hong Kong: The 1998 Legislative Council
 Election (Shiu-hing LO & Wing-yat YU), 68 pp. \$9.00

No. 5 - 1999 (154) **ISSN 0730-0107** **ISBN 0-925153-69-9**
 The ROC on the Threshold of the 21st Century: A Paradigm Reexam-
 ined (Edited by Chien-min CHAO & Cal Clark), 189 pp. \$24.00

No. 6 - 1999 (155) **ISSN 0730-0107** **ISBN 0-925153-70-2**
 Party Primaries in Taiwan: Trends, Conditions, and Projections in Can-
 didate Selection (Julian Baum and James A. Robinson), 39 pp. \$6.00

2000 Series

No. 1 - 2000 (156) **ISSN 0730-0107** **ISBN 0-925153-71-0**
 United States-Taiwan Relations: Twenty Years after the Taiwan Rela-
 tions Act (Edited by Jaw-Ling Joanne Chang & William W. Boyer),
 309 pp. Index. \$28.00
 (Hardcover edition: ISBN 0-925153-72-9) \$42.00

- No. 2 - 2000 (157)** **ISSN 0730-0107** **ISBN 0-925153-73-7**
 Taiwan's 2000 Presidential and Vice Presidential Election: Consolidating Democracy and Creating a New Era of Politics (John F. Copper), 66 pp. \$9.00
- No. 3 - 2000 (158)** **ISSN 0730-0107** **ISBN 0-925153-74-5**
 Legal Eligibility of Taiwan's Accession to GATT/WTO (CHO Hui-Wan), 22 pp. \$6.00
- No. 4 - 2000 (159)** **ISSN 0730-0107** **ISBN 0-925153-75-3**
 Russia's Northeast Asia Policy: Challenges and Choices for the 21st Century (Sharif M. Shuja), 22 pp. \$6.00
- No. 5 - 2000 (160)** **ISSN 0730-0107** **ISBN 0-925153-76-1**
 East Asia and the Principle of Non-Intervention: Policies and Practices (Linjun WU), 39 pp. \$7.00
- No. 6 - 2000 (161)** **ISSN 0730-0107** **ISBN 0-925153-77-X**
 The Association of South East Asian Nations' Confidence and Security Building with the People's Republic of China: Internal Constraints and Policy Implications (Kwei-Bo HUANG), 61 pp. \$9.00

2001 Series

- No. 1 - 2001 (162)** **ISSN 0730-0107** **ISBN 0-925153-78-8**
 Socio-economic Changes and Modernization in an Age of Uncertainty: Taiwan in the 1990s and Its Future Challenge (Wen-hui TSAI), 35 pp. \$7.00
- No. 2 - 2001 (163)** **ISSN 0730-0107** **ISBN 0-925153-79-6**
 Implementation of Taiwan Relations Act: An Examination after Twenty Years (Edited by Hungdah CHIU, Hsing-wei LEE and Chih-Yu T. WU), 267 pp. \$27.00
- No. 3 - 2001 (164)** **ISSN 0730-0107** **ISBN 0-925153-80-X**
 The Diplomatic War between Beijing and Taipei in Chile (Lin CHOU), 61 pp. \$9.00
- No. 4 - 2001 (165)** **ISSN 0730-0107** **ISBN 0-925153-81-8**
 Reforming the Protection of Intellectual Property: The Case of China and Taiwan in Light of WTO Accession (Andy Y. Sun), 46 pp. \$8.00
- No. 5 - 2001 (166)** **ISSN 0730-0107** **ISBN 0-925153-82-6**
 Arbitration of Commercial Disputes in China (Vai Io LO), 26 pp. \$6.00

No. 6 - 2001 (167)

ISSN 0730-0107

ISBN 0-925153-83-4

Building a Democratic State in Modernizing Taiwan: The 2001 Legislative Election and the Push for Pluralism (Wen-hui TSAI and George P. Chen), 24 pp.

\$6.00

2002 Series

No. 1 - 2002 (168)

ISSN 0730-0107

ISBN 0-925153-84-2

United States and Territorial Disputes in the South China Sea: A Study of Ocean Law and Politics (Yann-huei SONG), 321 pp.

\$35.00

No. 2 - 2002 (169)

ISSN 0730-0107

ISBN 0-925153-85-0

The Politics of Racial Discrimination in Hong Kong (Barry Sautman and Ellen Kneehans), 83 pp. (out of print)

\$10.00

No. 3 - 2002 (170)

ISSN 0730-0107

ISBN 1-932330-00-3

The Social and Political Bases for Women's Growing Political Power in Taiwan (Cal Clark and Janet Clark), 40 pp.

\$7.00

No. 4 - 2002 (171)

ISSN 0730-0107

ISBN 1-932330-01-1

The U.S.-Taiwan Free Trade Agreement: A Bridge for Economic Integration in the Asia-Pacific Region (Peter C.Y. Chow), 62 pp.

\$9.00

2003 Series

No. 1 - 2003 (172)

ISSN 0730-0107

ISBN 1-932330-02-X

Bringing People Back In: Collected Essays on Major Elections in Taiwan at the Turn of the 21st Century (Wen-hui TSAI), 125 pp.

\$18.00

No. 2 - 2003 (173)

ISSN 0730-0107

ISBN 1-932330-03-8

Taiwan: The Commercial State (Arthur I. Cyr), 81 pp. (out of print, please order No. 1 - 2005 (180) for a revised version of this issue)

\$10.00

No. 3 - 2003 (174)

ISSN 0730-0107

ISBN 1-932330-04-6

New Rules to the Old Great Game: An Assessment of the Shanghai Cooperation Organization's Proposed Free Trade Zone (Leland Rhett Miller), 25 pp.

\$6.00

No. 4 - 2003 (175)

ISSN 0730-0107

ISBN 1-932330-05-4

The Republic of China Legislative Yuan: A Study of Institutional Evolution (Thomas J. Bellows), 35 pp.

\$7.00

2004 Series

- No. 1 - 2004 (176)** **ISSN 0730-0107** **ISBN 1-932330-06-2**
Taiwan's 2004 Presidential and Vice Presidential Election: Democracy's Consolidation or Devolution? (John F. Cooper), 80 pp. \$10.00
- No. 2 - 2004 (177)** **ISSN 0730-0107** **ISBN 1-932330-07-0**
Peace, Reunification, Democracy and Cross-Strait Relations (Zhaohui HONG and Yi SUN), 16 pp. \$5.00
- No. 3 - 2004 (178)** **ISSN 0730-0107** **ISBN 1-932330-08-9**
Judicial Discretion in Dispensing with the Service of Process Requirement in Hong Kong under Order 45, Rule 7(7): Moving towards a Doctrine? (Simon Teng), 27 pp. \$7.00
- No. 4 - 2004 (179)** **ISSN 0730-0107** **ISBN 1-932330-09-7**
Taiwan's 2004 Legislative Election: Putting it in Perspective (John F. Copper), 75 pp. \$13.00

2005 Series

- No. 1 - 2005 (180)** **ISSN 0730-0107** **ISBN 1-932330-10-0**
Taiwan: The Commercial State (revised version of No. 2-2003 (173)) (Arthur I. Cyr), 81 pp. \$13.00
- No. 2 - 2005 (181)** **ISSN 0730-0107** **ISBN 1-932330-11-9**
Retracing the Triangle: China's Strategic Perceptions of Japan in the Post-Cold War Era (Danielle F. S. Cohen), 74 pp. (out of print) \$13.00
- No. 3 - 2005 (182)** **ISSN 0730-0107** **ISBN 1-932330-12-7**
Putting Things into Perspective: The Reality of Accountability in East Timor, Indonesia and Cambodia (Suzannah Linton), 90 pp. \$13.00
- No. 4 - 2005 (183)** **ISSN 0730-0107** **ISBN 1-932330-13-5**
Taiwan and the Soviet Bloc, 1949-1991 (Czeslaw Tubilewicz), 85 pp. \$13.00

2006 Series

- No. 1 - 2006 (184)** **ISSN 0730-0107** **ISBN 1-932330-14-3**
Japan's Changing Security Policy: An Overall View (Sharif Shuja), 32 pp. \$7.00
- No. 2 - 2006 (185)** **ISSN 0730-0107** **ISBN 1-932330-15-1**
China in ASEAN-LED Multilateral Forums (Serene Hung), 102 pp. \$14.00

No. 3 - 2006 (186) **ISSN 0730-0107** **ISBN 1-932330-16-X**
 East Mountain Tiger, West Mountain Tiger: China, the West, and
 "Colonialism" in Africa (Barry Sautman and YAN Hairong),
 77 pp. (out of print) \$13.00

No. 4 - 2006 (187) **ISSN 0730-0107** **ISBN 1-932330-17-8**
 Taiwan's 2006 Metropolitan Mayoral and City Council Elections and
 the Politics of Corruption (John F. Copper), 65 pp. \$12.00

2007 Series

No. 1 - 2007 (188) **ISSN 0730-0107** **ISBN 1-932330-18-6**
 National Identity, Ethnic Identity, and Party Identity in Taiwan (Chang-
 Yen TSAI), 34 pp. \$8.00

No. 2 - 2007 (189) **ISSN 0730-0107** **ISBN 1-932330-19-4**
 Combating Corruption Singapore-Style: Lessons for Other Asian Coun-
 tries (Jon S.T. Quah), 56 pp. \$12.00

No. 3 - 2007 (190) **ISSN 0730-0107** **ISBN 1-932330-20-8**
 The Status of Customary International Law, Treaties, Agreements and
 Semi-Official or Unofficial Agreements in Law of the Republic of
 China on Taiwan (Hungdah CHIU and Chun-I CHEN), 31 pp. \$8.00

No. 4 - 2007 (191) **ISSN 0730-0107** **ISBN 1-932330-21-6**
 Rape Myths in American and Chinese Laws and Legal Systems: Do
 Tradition and Culture Make the Difference? (Marietta Sze-chie
 Fa), 109 pp. \$16.00

2008 Series

No. 1 - 2008 (192) **ISSN 0730-0107** **ISBN 1-932330-22-4**
 Taiwan's 2008 Presidential and Vice Presidential Election: Maturing
 Democracy (John F. Copper), 90 pp. \$15.00

No. 2 - 2008 (193) **ISSN 0730-0107** **ISBN 1-932330-23-2**
 The Political Economy of South Korea: Economic Growth, Democrati-
 zation, and Financial Crisis (Uk HEO, HOUNGcheul JEON, Hayam
 KIM and Okjin KIM), 24 pp. \$7.00

No. 3 - 2008 (194) **ISSN 0730-0107** **ISBN 1-932330-24-0**
 Korean Dispute over the Northern Limit Line: Security, Economics, or
 International Law? (Terence Roehrig), 59 pp. \$12.00

No. 4 - 2008 (195) **ISSN 0730-0107** **ISBN 1-932330-25-9**
 Evolving On-Line Empowerment: The Manchu Identity Revival Since
 the 1980s (BAI Lian), 48 pp. \$10.00

2009 Series

- No. 1 - 2009 (196)** **ISSN 0730-0107** **ISBN 1-932330-26-7**
Taiwan at a Turning Point (Edited by Seyom Brown, Cal Clark, Hiroki Takeuchi, and Alex Tan), 98 pp. \$18.00
- No. 2 - 2009 (197)** **ISSN 0730-0107** **ISBN 1-932330-27-5**
The Background, Principles and Core Contents of the Real Right Law of The People's Republic of China (ZHU Yan), 39 pp. (out of print) \$8.00
- No. 3 - 2009 (198)** **ISSN 0730-0107** **ISBN 1-932330-28-3**
"All that Glitters Is Not Gold": Tibet as a Pseudo-State (Barry Sautman), 86 pp. \$15.00
- No. 4 - 2009 (199)** **ISSN 0730-0107** **ISBN 1-932330-29-1**
Positive Equilibrium in U.S.-China Relations: Durable or Not? A time of "testing" in Sino-American Relations (Robert Sutter), 52 pp. \$12.00

2010 Series

- No. 1 - 2010 (200)** **ISSN 0730-0107** **ISBN 1-932330-30-5**
An Insight into Insider Trading in Greater China (Greg Tzu Jan Yang), 61 pp. \$14.00
- No. 2 - 2010 (201)** **ISSN 0730-0107** **ISBN 1-932330-31-3**
Taiwan's Anti-Corruption Strategy: Suggestions for Reform (Jon S.T. Quah), 111 pp. \$18.00
- No. 3 - 2010 (202)** **ISSN 0730-0107** **ISBN 1-932330-32-1**
The East Asia Summit and the Regional Security Architecture (Ralf Emmers, Joseph Chinyong Liow, and See Seng TAN), 52 pp. \$12.00
- No. 4 - 2010 (203)** **ISSN 0730-0107** **ISBN 1-932330-33-X**
Taiwan's 2010 Metropolitan City Elections: An Assessment of Taiwan's Politics and a Predictor of Future Elections (John F. Copper), 67 pp. \$15.00

2011 Series

- No. 1 - 2011 (204)** **ISSN 0730-0107** **ISBN 1-932330-34-8**
Legal Aid and the Rule of Law in the People's Republic of China (Mark Jia), 63 pp. \$15.00

No. 2 - 2011 (205) **ISSN 0730-0107** **ISBN 1-932330-35-6**
 Mahathir's Successors: Sharpening Dilemmas in Malaysian Politics
 (William Case), 72 pp. \$16.00

No. 3 - 2011 (206) **ISSN 0730-0107** **ISBN 1-932330-36-4**
 In Pursuit of Gradual Stabilization and Peace Dividends: Cross-Taiwan
 Strait Relations and Their Influence on the Asia Pacific (Kwei-Bo
 HUANG), 54 pp. \$13.00

No. 4 - 2011 (207) **ISSN 0730-0107** **ISBN 1-932330-37-2**
 Institutional Design and Development in the ROC (Taiwan): A Critical
 Review of the Thoughts of SUN Yat-sen and the Global Develop-
 ment of the Ombudsman System (GER Yeong-kuang), 59 pp. \$14.00

2012 Series

No. 1 - 2012 (208) **ISSN 0730-0107** **ISBN 1-932330-38-0**
 Taiwan's 2012 Presidential/Vice Presidential and Legislative Elections:
 Assessing Current Politics and Charting the Future (John F. Cop-
 per), 85 pp. \$17.00

No. 2 - 2012 (209) **ISSN 0730-0107** **ISBN 1-932330-40-2**
 Insider Trading in China: Compared with Cases in the United States
 (Greg Tzu Jan Yang), 65 pp. \$16.00

No. 3 - 2012 (210) **ISSN 0730-0107** **ISBN 1-932330-39-9**
 The Chinese Are the Worst?: Human Rights and Labor Practices in
 Zambian Mining (Barry Sautman and YAN Hairong), 100 pp. \$20.00

No. 4 - 2012 (211) **ISSN 0730-0107** **ISBN 1-932330-41-0**
 The State of Play on International Piracy and Anti-Counterfeiting Strat-
 egies (Andy Y. Sun), 59 pp. \$16.00

2013 Series

No. 1 - 2013 (212) **ISSN 0730-0107** **ISBN 1-932330-42-9**
 Sustaining the Triangular Balance: The Taiwan Strait Policy of Barack
 Obama, XI Jinping, and MA Ying-jeou (Dean P. Chen), 83 pp. \$18.00

No. 2 - 2013 (213) **ISSN 0730-0107** **ISBN 1-932330-43-7**
 China Under the New Leadership (Hsin-Chi KUAN), 70 pp. \$17.00

No. 3 - 2013 (214) **ISSN 0730-0107** **ISBN 1-932330-44-5**
 Political Economy of Vietnam: Market Reform, Growth, and the State
 (Joshua M. Steinfeld and Khi V. THAI), 72 pp. \$17.00

No. 4 - 2013 (215)

ISSN 0730-0107

ISBN 1-932330-45-3

Minimizing Corruption in China: Is This an Impossible Dream? (Jon S. T. Quah), 99 pp. \$20.00

2014 Series

No. 1 - 2014 (216)

ISSN 0730-0107

ISBN 1-932330-46-1

The Mutual Non-Denial Principle, China's Interests, and Taiwan's
Expansion of International Participation (Wei-chin LEE), 55 pp. \$15.00

No. 2 - 2014 (217)

ISSN 0730-0107

ISBN 1-932330-47-X

Seeking Common Ground While Keeping Differences: "Using the Case
of Cross-Strait Relations as a Case" (Charles Chong-han Wu),
51 pp. \$15.00

No. 3 - 2014 (218)

ISSN 0730-0107

ISBN 1-932330-48-8

Indonesia Beyond *Reformasi*: *Necessity* and the “De-centering” of
Democracy (Leonard C. Sebastian, Jonathan Chen and
Adhi Priamarizki), 79 pp. \$18.00

No. 4 - 2014 (219)

ISSN 0730-0107

ISBN 1-932330-49-6

Taiwan's 2014 Nine-in-One Election: Gauging Politics, the Parties, and Future Leaders (John F. Copper), 81 pp.	\$19.00
---	---------

2015 Series

No. 1 - 2015 (220)

ISSN 0730-0107

ISBN 1-932330-50-X

Hunting the Corrupt “Tigers” and “Flies” in China: An Evaluation of
X1 Jinping’s Anti-Corruption Campaign (November 2012 to March
2015) (Jon S.T. Quah), 98 pp. \$22.00

No. 2 - 2015 (221)

ISSN 0730-0107

ISBN 1-932330-51-8

Localists and "Locusts" in Hong Kong: Creating a Yellow-Red Peril Discourse (Barry Sautman and YAN Hairong), 94 pp. \$22.00

No. 3 - 2015 (222)

ISSN 0730-0107

ISBN 1-932330-52-6

Peaceful Settlement of Disputes in the South China Sea through Fisheries Resources Cooperation and Management (Kuan-Hsiung WANG), 45 pp.	\$17.00
--	---------

No. 4 - 2015 (223)

ISSN 0730-0107

ISSN 1.932330.53.4

The Recent Development of China's Anti-monopoly Law on Standard Setting Organization's Patent Pooling Arrangement and the Issues of Incorporating Patent Misuse Doctrine as the Antitrust Review Standard (Nigel Naihung Lee), 53 pp.	\$18.00
---	---------

2016 Series

- | | | |
|---|-----------------------|---------------------------|
| No. 1 - 2016 (224) | ISSN 0730-0107 | ISBN 1-932330-54-2 |
| Taiwan's 2016 Presidential/Vice Presidential and Legislative Election:
Reflections on the Nature of Taiwan's Politics and Shifts Therein
(John F. Copper), 79 pp. | | \$20.00 |
| No. 2 - 2016 (225) | ISSN 0730-0107 | ISBN 1-932330-55-0 |
| Taiwan and Southeast Asia: Opportunities and Constraints of Continued Engagement (JING Bo-jiun), 86 pp. | | \$21.00 |
| No. 3 - 2016 (226) | ISSN 0730-0107 | ISBN 1-932330-56-9 |
| China's Epochal Case: A Tale of Two Ships (James A.R. Nafziger),
50 pp. | | \$19.00 |
| No. 4 - 2016 (227) | ISSN 0730-0107 | ISBN 1-932330-57-7 |
| Cyber Wrongs in Greater China (Greg Tzu Jan Yang), 46 pp. | | \$18.00 |

MARYLAND STUDIES IN EAST ASIAN LAW AND POLITICS SERIES

(The following books are published under the auspices or co-auspices of the East Asian Legal Studies Program of the University of Maryland School of Law. The views expressed in each book reflect only those of the author. All books published in hard cover edition, unless otherwise indicated.)

1. Hungdah CHIU, *China and the Taiwan Issue*. New York: Praeger Publishers, A Division of Holt, Rinehart and Winston/CBS, Inc., 1979. 295 pp. (Now distributed by the Greenwood Press)
ISBN 0-03-048911-3 \$49.95
2. Hungdah CHIU, *Agreements of the People's Republic of China, A Calendar of Events 1966-1980*. New York: Praeger Publishers, A Division of Holt, Rinehart and Winston/CBS, Inc., 1981. 329 pp. (Now distributed by the Greenwood Press)
ISBN 0-03-059443-X \$49.95
3. David Salem, *The People's Republic of China, International Law and Arms Control*. Baltimore, Maryland: University of Maryland School of Law OPRSCAS*, 1983. 325 pp.
ISBN 0-942182-59-6 \$15.00
4. Ying-jeou MA, *Legal Problems of Seabed Boundary Delimitation in the East China Sea*. Baltimore, Maryland: University of Maryland School of Law, 1984. 308 pp.
ISBN 0-942182-63-4 \$15.00
5. Hungdah CHIU and Shao-chuan LENG, editors, *China: 70 Years After the 1911 Hsin-hai Revolution*. Charlottesville, Virginia: University Press of Virginia, 1984. 600 pp.
(Published under the co-auspices of the Committee on Asian Studies, University of Virginia.)
ISBN 0-8138-1027-7 \$35.00
6. Shao-chuan LENG and Hungdah CHIU, *Criminal Justice in Post-Mao China*. Albany, New York: State University of New York Press, 1985. 325 pp.
(Published under the co-auspices of Committee on Asian Studies, University of Virginia.)
ISBN 0-87395-950-7 (hardcover) \$74.50
ISBN 0-87395-948-5 (paperback) \$24.95

* Occasional Papers/Reprints Series in Contemporary Asian Studies, Inc. (It has been changed to Maryland Series in Contemporary Asian Studies, MSCAS), 500 West Baltimore St., Baltimore, Maryland 21201-1786. (Tel. 410-706-3870)

7. Jaw-ling Joanne CHANG, *United States-China Normalization: An Evaluation of Foreign Policy Decision Making*. Baltimore, Maryland: University of Maryland School of Law OPRSCAS, 1986. 246 pp. (Copublished with Monograph Series in World Affairs, University of Denver)
ISBN 0-942182-78-2 \$12.00
8. Lester Ross and Mitchell A. Silk, *Environmental Law and Policy in China*. Westport, CT: Greenwood Press (Quorum Books), 1987. 449 pp.
ISBN 0-89930-204-1 \$75.00
9. Hungdah CHIU, Y.C. JAO and Yuan-li WU, editors, *The Future of Hong Kong: Toward 1997 and Beyond*. Westport, CT: Greenwood Press (Quorum Books), 1987. 262 pp.
ISBN 0-89930-241-6 \$55.00
10. Ray S. Cline and Hungdah CHIU, eds., *The United States Constitution and Constitutionalism in China*. Washington, D.C.: U.S. Global Strategy Council, 1988. Distributed by OPRSCAS, 166 pp. Paper. \$8.00
11. Winston L.Y. YANG and Marsha L. Wagner, eds., *Tiananmen: China's Struggle for Democracy—Its Prelude, Development, Aftermath, and Impact*. Baltimore, Maryland: University of Maryland School of Law OPRSCAS, 1990. 314 pp. Index
ISBN 0-925153-08-7 \$14.00
12. Mitchell A. Silk, ed., *Taiwan Trade and Investment Law*. Hong Kong: Oxford University Press, 1994. 693 pages.
ISBN 0-19-585289-3 \$59.00

ORDER FORM

Mail this order form to Maryland Series in Contemporary Asian Studies,
University of Maryland School of Law, 500 West Baltimore Street,
Baltimore, Maryland 21201-1786, U.S.A. Or e-mail to eastasia@law.
umaryland.edu or fax to (410)706-1516

Check One:

☐ Please Send:

ISBN

Title

No. of Copies

☐ Please start my subscription of the MSCAS: Starting year _____

Subscription price is U.S. \$50.00 per year for 4 issues in the U.S. and
\$60.00 for Canada, Mexico or overseas (regardless of the price of
individual issues).

My check of U.S. \$ _____ is enclosed.
_____ copy(s) of invoice/receipt required. (Institution/
library may request billing before making payment)
For individual order, please add postage/handling of \$8.00 for one
copy and \$4.00 for each additional copy. Make checks payable to
MSCAS.

Please send books to:

Contact Name

Corporation/Library/Institution

Address (Please include zip code)

Country
