

---

## 5. Throttle the Intellectual Property Criminal Infringement

### - Trend of and Countermeasures against the Crimes of Internet Infringement of Rights

WANG Zhiguang, Deputy Director, Intellectual Property Division,  
Economic Crime Investigation Department, Ministry of Public Security of China

---

#### Overview

The uprush of an undercurrent of Internet IPR infringement has started on the Internet because of the extensive applications of the Internet and the dramatic changes of digital technologies day by day. In particular, the characteristics of “Un-centralized” and “Digitalized” result in the further expansion of crimes in IPR infringement, which is of characteristics of “Organized”, “Cyberized” and “Internationalized”.

#### Main Types of Internet Infringement

Committing the “Traditional” Crimes of IPR Infringement through the Internet.

Selling infringement commodities and medicines through Internet: lawless elements operate websites on the Internet and distribute the information of manufacturing and sales of fake products to every corner of the world, which causes an isolated local issue of IPR infringement being evolved into a worldwide threat.

Selling infringed digital information through Internet. Sales and downloads of pirate DVD or VCD movies and MP3 music through or from Internet have become an important part of the lives of many netizens.

#### New Forms of Internet Crimes

Framing of Internet application services for infringement: including the special Internet application services such as private services for internet games and internet digital libraries.

Bypassing the protection technical measures for digital information and application programmes: including the software decoding patch, game extension and decoding of the protection technical measures for digital copyright. Moreover, some are hired by pirate criminal groups to specially engage in software decoding, which worsens the situation of infringement crimes.

Infringement of trademark and patents in the field of information network technologies: such as infringement of software patent right and malicious registration of domain names.

#### Core Instruments for Internet Infringement and Pirate

**Commercial websites** including B2B and B2C which are used as instruments for distribution of pirate works and spreading information of infringing commodities; even worse, the same is used by many lawless elements as accomplice to seek for suppliers and purchasers to form an international “syndicate”.

**Community forum**: it is most common to see that HTTP or FTP is manipulated for provisions of downloading pirate software, music and movie in a hidden form. Due to the open nature of the Internet, these pirate websites or FTP sites have gathered a lot of overseas or remote servers.

**“Decoding Websites”**. Some netizens fans and computer professionals collected and made various decoding software, decrypting instruments or encryptions and pasted the same on their websites or web pages to exclusively provide pirate software.

**“Private Services”**. To date, it is identified by China that there are certain types as follows: i) domestic “private services”, which are mainly set up by cybercaves or senior Internet users; ii) commercial “private services” and iii) alliance of “private services”.

#### BT Technologies and Analysis of Legal Responsibilities

**“Peer to Peer”**: which uses the direct transition of information and services between individuals or equivalent equipment on the Internet to realize the direct share of document, directories and even the entire hard disk among the Internet users.

BT is an abbreviation for “BIT TORRENT” (“Point-to-point File Sharing”) technology, of which, the core remains P2P technology but uses the principles of “multi-points to multi-points”.

The first criminal case concerning BT download in the world - Chen Naiming Case, Hong Kong.

Unresolved issues: BT issues will continue catching extensive attention.

### **Characteristics of Internet Infringement and Pirate and Analysis of Difficulties in Investigation**

Because of the “infinite” nature of the Internet, it is very difficult to identify the clues for Internet infringement and pirate cases.

Because of the “open” nature of the Internet, trans-region and trans-country become the typical characteristics of these crimes.

Legislation of each country, legislations concerning the enforcement of relevant laws in particular, lags behind the development of technologies.

The investigation mode of and technologies used by the law enforcement organs in each country are not adapted to the current trend of the crimes.

Lack of supervision and management as well as industrial associations’ self-discipline in each country.

### **Trend and Frontier of the Law Enforcement in Each Country**

Law enforcement organs in some countries and regions have started to focus on the monitoring and control of Internet IPR infringement crimes.

China has defined the criteria for the conviction and punishment of infringement and pirate crimes; and provisions that the authors, performers and producers of sound and video recordings are entitled to the right of communication through information Internet are added to the Copyright Law.

China’s public security organs will severely punish the criminal activities of online IPR infringement: i) the public security organ at each level set up a coordination leading group on punishment of IPR infringement crimes to activate all resources of various departments, such as economic crime investigation, social security and network supervision, for the purpose of implementing more complete and firmer punishment against crimes of infringement; ii) together with the Administration for industry and commerce, copyright and custom authorities new transition and cooperation provisions are to be instituted to establish the new strategies and coordinating mechanism for punishing crimes of infringement; and iii) the special program of “Mountain Eagle II” is arranged and deployed, which focuses on online crimes and covers all the crimes in terms of infringement of IPR.

### **Suggestions to Tighten the Punishment of Internet Infringement Crimes**

It is for sure that the criminal activities in infringement of IPR, which rely upon high intelligence and high technologies, will be more covert, more professional and more organized. The law enforcement organ in each country, as well as the industrial associations and right owners shall form more effective action strategies.

First of all, to institute and enforce firmer and more effective laws. Relevant laws shall be in place based on the means and characteristics of crimes on online IPR infringement.

Secondly, to reinforce international cooperation in terms of law enforcement and reform the modes of law enforcement and cooperation and to adhere to the principles of “Accurate Punishment” and “Entire Course Punishment”; and to destroy the transnational criminal network and the infringement and pirate wickiups and to effectively punish the hidden principals.

Thirdly, to enable law enforcers grasp basic knowledge of IPR and Internet as well as the investigation skills via implementation of educations and trainings so as to improve the law enforcement capacities in terms of evidence collection, investigations and prosecution.

Fourthly, to establish special law enforcement contingents, consolidate the monitoring and control of the Internet and improve the professional competence and punishment efficiency of the law enforcement contingents.

Fifthly, unless the law enforcement organs, various industrial associations and enterprises strengthen the supervision and management and self-discipline, in particular the efforts in furnishing the consciousness of intellectual property protection with Internet users, the Internet won’t become a Pure Land.

*(Original Text in Chinese)*

## Throttle the Intellectual Property Criminal Infringement

--- Trend of and Countermeasures against the Crimes of Internet Infringement of Rights

Zhiguang Wang

Department of Economic Crime Investigation,  
Ministry of Public Security

## “The Strategic Channel”

### --- The Internet

- It makes the use of counterfeit and pirated products more widespread, and makes them flow even faster to all parts of China and even overseas
- It enables unlawful elements in different regions and countries to form a criminal chain involving “integrated production, supply and sales”
- The governments, law enforcement institutions and societies of each country are confronting new challenges

## Overview

- The Internet crisis --- The current state of rights infringement and pirating crimes on the Web
- The core tools of rights infringement and pirating on the Web
- Analysis of Bit Torrent (BT) technology and legal liability
- Characteristics of Internet Infringement and Pirate and Analysis of Difficulties in Investigation
- Trends and frontier of the law enforcement in each country
- Suggestions for strengthening the fight against the crime of rights infringement on the Internet

### I. The Internet Infringement

--- The current state of the crimes of rights infringement and pirate versions crimes on the Web

----- If you are able to access the Internet, then you are able to take anything that can be transformed into byte or data streams and turn it into a tool for or the object of rights infringement and pirate versions

### 1. Products and medicines

- Approximately 5% to 7% of the products worldwide are counterfeit
- As much as 10% of the medicines worldwide are fake
- Sales of counterfeit goods in New York in 2003 was 23 billion US dollars

### 2. Music

- MP3.com paid compensation of 160 million US dollars to Warner and EMI, and announced the end of the free MP3 era.
- Pirating caused worldwide record sales to slide from 38.0 billion US dollars in 1998 to 30.0 billion US dollars in 2003

### 3. Software

- The majority of software available can be found on the Web
- 35% of software worldwide in 2004 is pirated

### 4. Cyber games

- “Private servers” have become a kind of massive illegal “industrial alliance”
- The illegal cyber game industry is in its initial stage of formation, and the amount of money involved in this illegal business is as high as more than 100 million Chinese *yuan*
- The Chinese cyber game industry is confronting a severe test

## II. Core Instruments for Internet Infringement and Pirate

### 1. Commercial websites

- At the same time as these promote the widespread dissemination of information and products, they also play the role of disseminating pirated works and spreading information about counterfeit products, to the point where unlawful elements seek to build an integrated supply chain and create accomplices in an international “syndicate”

### 2. Community forums:

These provide a variety of information about rights infringement and pirate versions, search engines and linked forum web pages

### 3. “Decoding” websites

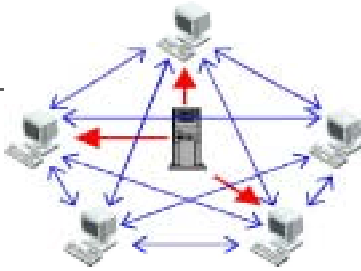
These collect and produce various kinds of cracking software, decryption tools or cipher keys, etc., and make them available on the website or its web pages

### 4. “Private services”

- Domestic “private services”
- Commercial “private services”
- Alliance of “private services”

## III. BT Technologies and Analysis of Legal Responsibilities

- “Peer to Peer”: which uses the direct transition of information and services between individuals or equivalent equipment on the Internet to realize the direct share of document, directories and even the entire hard disk among the Internet users.
- Napster, Grokster, KaZaA, Morpheus, eDonkey
- The BT core is still P2P technology



Owing to the fact that it involves downloading by multiple connections and mutual sharing, the more people that download a certain file, the lighter the burden is on the uploader, and the faster the downloads are for everyone

**The first criminal case concerning BT download in the world**  
 --- Chen Naiming Case in Hong Kong

- In January 2005, Chen Naiming, a resident of Hong Kong, was arrested by Hong Kong Customs since he had used BT to distribute three Hollywood films including *Daredevil*.
- On November 7, Hong Kong's Special District Court finally sentenced Chen Naiming to 3 months' imprisonment.
- This case, which was the first time in the world that the act of BT rights infringement was judged to be a crime by a court, was also the first time that an individual user of the Internet was held criminally liable.

**The problems with Chen Naiming's criminal liability**

- The TRIPs Agreement: Each member shall stipulate at least the criminal procedure or punishment to be utilized for deliberately counterfeited trademark or piracy cases that take place on a commercial scale
- Does this case constitute commercial scale
  - "Deliberately violates intellectual property rights and results in economic losses to the right holder"
  - "Causes economic losses to the right holder"
  - "Deprives another person of the of the ability to make a profit"
- An unfinished but deeply significant decision

**IV. Characteristics of Internet Infringement and Pirate and Analysis of Difficulties in Investigation**

**(1) Because of "infinite" nature of the Internet, concealment is the prominent characteristic of cyber crime**


- There were 9 cases of network crime in China in 1986, 2,700 cases in 2000 and 4,500 cases in 2002, but it is reported that only 1% of such crimes are discovered
- The information about legal vs. illegal and official vs. pirate versions is voluminous, with good and bad mixed together, and this in effect creates a kind of concealment
- Criminal activities can be completed in a few seconds' time, and can rapidly spread and expand without discovery

**(2) Because of the "open" nature of the Internet, trans-region and trans-country become the typical characteristics of these crime**

- The Internet is used by unlawful elements as a tool for finding and disseminating information about rights infringement and pirate versions, and has created many criminal networks that are seemingly loosely connected but whose ties are wide-ranging
- Now that China is serving as a global factory, some unlawful elements have also begun to seek manufacturers and agents inside China

**Problems with the conflict over court jurisdiction**  
 --- Who has jurisdiction over cyber crime?

- The Russian company ElcomSoft cracked the code for Adobe's document reader program and provided downloads on the Web
- The US Department of Justice accused ElcomSoft and its chief technician Skylaro of illegally developing the above-described software based on the Digital Millennium Copyright Act (DMCA)
- Skylaro planned to attend a conference in Las Vegas and was arrested by the Federal Bureau of Investigation, and faced a fine of 2.25 million US dollars and 25 years in jail
- The US Federal Court for the Northern California District announced that ElcomSoft was innocent and released him




### (3) The technical nature of cyber crime is strong, and it involves a wide range of fronts, and thus the degree of difficulty in investigating and proving cyber crime is relatively great.

- The virtual network space has limitless expandability, and the forms and techniques of rights infringement and piracy on the Web change ceaselessly. This causes relatively great difficulty for investigative authorities in investigating and breaking cases and collecting evidence.
- I will use the "Warez" Web piracy case in the United States as an example



### "Warez"

- **Second level: Technical and administrative personnel**
  - \* Provide new products
  - \* Measures for cracking the copyright protection
- **Third level: High-level couriers**
  - Distribute pirated software on the in-house FTP server
- **Fourth level: Low-level secondary couriers**
  - \* Send to public Internet sites
  - \* Maximum record:
    - Transmitting to 10,000 servers in 6-12 hours
- **Fifth level: Worldwide pirate version users**
  - \* 10,000 servers send several million copies
  - \* P2P, fee-based servers, auction websites



### (4) Legislation lags behind the development of technology, and this results in conflicts and omissions in legislation and law enforcement

- The change from traditional hard copies to digitalization has caused huge changes in legal concepts, values, commercial models, etc.
- It raises a series of basic problems, for example what is legal (i.e., how to legitimately seek profits), what is beneficial for promoting innovation, etc., but the answers are still not clear
- There is still an inadequate legal foundation for attacking crimes like setting up services for rights infringing network applications, by passing electronic information and technical measures for protecting application programs, etc.



## V. Trends and frontier of the law enforcement in each country

### 1. On the legislative front

- Continue to widen the scope of adjustment of intellectual property laws to provide still more protection to digitalized information like music, films, texts, etc.
- Pass new laws to protect the security measures for new technologies
- The European Council has enacted Directive 2001/29/EC, that is, the European Union Copyright Directive (EUCD)
- The question of how to enact domestic legislation according to the EUCD, for example, the question of how to concretely prescribe technical measures like protective encryption, digital watermarks and limited copying, and the question of how to formulate in actual practice the related definitions, exemptions, sanctions and compensation, are still awaiting the examination of the member states of the EU for adoption of legislation and enforcement in actual practice




### 2. On the law enforcement front

- The US Department of Homeland Security and Justice Department have respectively established divisions in charge of computer crimes, and attacking crimes involving infringement of intellectual property rights on the Web will serve as their chief duty in the future



### China attacks crimes involving infringement of intellectual property rights on the Web

- In December 2004, the Supreme People's Court and Supreme People's Procuratorate explained that they had clarified criteria whereby the punishment fits the crime for crimes of rights infringement and piracy.
- The new Copyright Law increases the provisions relating to writers, performers and sound and video recording artists sharing information network dissemination rights
- Alliances of the Copyright Department, Ministry of Industry, etc., will launch a special campaign against "private servers" and online game cheats (OGC).
- In 2005, public security organs investigated and disposed of 55 cases of use of the Internet to sell counterfeit goods and pirated products
- In July 2005, the Investigation Squad of the Putuo Branch of the Shanghai Municipal Public Security Bureau broke the case of Tang-cun You and others who had established the Chuanqi 3 "private server," and were providing a game service illegally on the Internet




### 2006 --- Chinese Public Security Organs

- China established a small group for coordinating and leading the attack on crimes involving infringement of intellectual property rights, and mobilized the resources of the Economic Crimes Investigation, Public Order, Internet Supervision and other divisions and committed them to the task of protecting intellectual property rights
- It launched the special campaign "Mountain Eagle 2" to attack crimes involving infringement of intellectual property rights, with criminal cases of the sale of counterfeit products and pirated products using the Internet as the focus of the special campaign
- It has already investigated and broken close to 80 cases wherein the Internet was used to infringe on intellectual property rights



### Opening a "Second Battlefield" for attacking crimes involving infringement of intellectual property rights

- Owing to the spur of huge profits and the existence of the consumer markets of each country in the world, criminal activities involving rights infringement and piracy are still rampant on a global scale, and criminal activities involving infringement of intellectual property rights on the Web are becoming more and more serious.
- The law enforcement institutions of each country must raise further their capacity and level in attacking crimes involving infringement of intellectual property rights on the Web, formulate more effective action strategies, expand the scope of investigation to the whole criminal network, and recover the criminal proceeds — only then can they completely cut off the ability to reproduce





### vi. Suggestions to tighten the punishment of Internet infringement crimes

#### (1) Strengthen the ability to monitor information about rights infringement crimes on the Internet

- Take the initiative in collecting, studying and evaluating information about rights infringement crimes on the Internet and the key businesses involved in the same, and investigate and break open some major multinational criminal cases whose circumstances are particularly odious, and thereby curb the rampant tendency of Web-based rights infringement crimes.



- Widely collect leads to cases through the online website for informing about violations and crimes:  
**[www.cyberpolice.cn](http://www.cyberpolice.cn)**



#### (2) Strengthen the ability for coordinated operations across regions and across governmental departments

- Establish a mechanism for coordinated operations, strengthen exchanges of information and intelligence, integrate leadership, and unite in the fight
- Reveal the entire criminal network and the organizational strategists behind the scenes, and subject them to the severest punishment of the law



#### (3) Strengthen cooperation in international law enforcement

- Insist on the policies of "precise attacks" and "thorough attacks," and mount a full-scale attack on the links involved in counterfeit criminal activities, such as producing counterfeit labels, production, sales, customs declaration and export, retails sales, etc., and thereby deal a lethal blow to multinational criminal activities and networks



#### (4) Strengthen education and training of law enforcement personnel

- Ensure that law enforcement personnel have basic knowledge about and investigative techniques for intellectual property rights and the Internet
- Understand the strategies and investigative models for attacking crimes involving infringement of intellectual property rights, provide training in case investigation, use of intelligence and ascertaining the data, and raise law enforcement capabilities in collecting information and investigating cases

#### (5) Perfect the related laws

- Traditional intellectual property rights crimes have further developed and spread on the Internet and moreover become more heterogeneous, and the criminal code currently in force has no way to adapt to the features of cyber crime
- At present, public security organs are energetically promoting the work of revising criminal legislation about cyber crime so that it is suited to the needs of attacking the circumstances of rights infringement crimes on the Web
- Of these, the focus of our proposals for revisions are the new kinds of crimes produced by the diversification on the Web of the crimes of infringement of copyrights, trademarks, patent rights and commercial secrets.

#### Jointly return the Internet to the state of a "Pure Land"

- Strengthen cooperation with copyright departments and rights holders
- Guide those using the Internet so that they strengthen their self-restraint, and do not use or disseminate pirated products and do not sell goods that infringe on others' rights
- Raise the consciousness of the entire society about protecting intellectual property rights



## Thank You!

Zhi-guang Wang  
Intellectual Property Rights Office  
Department of Economic Crime Investigation  
Ministry of Public Security  
Tel: (8610) 65203947  
cell: (86) 13910535176  
E-mail: mpswang@163.com

*(Original Text in Chinese)*

#### A question from the participants to Mr. WANG

Q. I'm from the Changchun Municipal Copyright Bureau. We once discovered over 20,000 pirated optical discs, but when we handed them over to the public security authorities they asked us to provide evidence of infringement. But the discs that we discovered in that case involved many different fields, so there was no way for us to track down all the right holders and contact them for verification. When we deal with criminal copyright cases of this sort, do we have to bear such a heavy burden of proof?

A. In copyright crime detection and law enforcement work, we do indeed frequently find it difficult to determine infringement amounts and sales amounts or obtain a conviction due to the lack of sales records. In addition, the difficulty of contacting right holders also makes it hard for public security organs (police) to obtain evidence of infringement. We generally recommend investigating such cases as illegal business operations, using the standard for burden of proof that applies in cases of illegal business operations. This lowers the difficulty of investigation a bit and lightens the burden of proof a bit.