ISSN 2343-4724

Journal of Legal Studies

Volume 1 Winter 2016

Nordic Journals

This publication was entitled the *Journal of Legal Studies*.

ISSN 2343-4724

The *Journal of Legal Studies* provides a forum for legal studies. The *Journal* welcomes manuscripts for possible publication from authors both within and outside the legal profession. Send correspondence and manuscripts by e-mail. Submissions should be typewritten and footnotes and references should conform with *Publication Manual of the American Psychological Association*®.

Subscription Prices (online): EUR €29.00

The *Journal of Legal Studies* is accessible at:

http://jls.pruna.eu

Email: submissions@pruna.eu

Published in Helsinki, Finland

Available online at jls.pruna.eu
Journal of Legal Studies
Journal of Legal Studies, 2016, 1–36
Received: 1 May 2016. Accepted: 3 June 2016. Published: 19 October 2016

Taxonomy of Cybercrime

Xingan LI♣

Abstract: The purpose of this article is to propose an approach for classifying cybercrime based on review of previous research. The article expands the roles of data processing systems in cybercrime and divides cybercrime into seven categories. Data processing systems in use as mass media, operating mechanism, place of occurrence, transfer channel, targeted object, and multiple-purpose instrument, or used in the preparation for other crimes and theoretically expands the roles of data processing systems in cybercrime.

Keywords: Cybercrime; Cyberspace; Classification; Role of information; Informatics

Introduction

More than ever before, cybersecurity is confronted with the threat of cybercrime in the 21st century (Li 2016). Although the pervasive use of data

♣ Associate Professor, Tallinn University, School of Governance, Law and Society.

processing systems is accompanied by a wide range of social problems, and the countermeasures necessitate mobilizing a broad variety of legal remedies, this article will primarily be concentrating on the criminal phenomenon accompanying data processing systems and on the deterrence framework revolving around but not limited to criminal law. Therefore, the main task facing us is to determine the scope of the topic, through defining the subject-matter "cybercrime" based on an improved version of my previous taxonomical framework (Li 2008a).

Alternative definitions of cybercrime have emerged over the years as the users and abusers of computers expand into new areas. There is neither a unified definition, nor a commonly accepted method of classification. The definition and classification methods are so diversified that it is impossible to sketch the scenario of cybercrime by using a single standard (Wasik 1991, p. 1). The present rampancy of cybercrime can in part be understood as the product of weak legal deterrence.

The purpose of this article is to propose an approach for classifying cybercrime based on review of previous research. Following this introduction, the article goes on to analyze previous notions on computer crime, giving brief evaluation of deficiencies of traditional definitions. The article will also interpret the socio-legal meaning of the label "cyber". In the latter part, this article will advocate the use of a unified broad definition of cybercrime, in order to reach a consensus as great as possible, reform both substantive and procedural criminal law and provide effective protection for the information society. The article also proposes to classify cybercrime according to the roles of data processing systems into seven categories, data processing systems as target, tool, media, route, place, means of crime, and used in preparation for further offences.

Taxonomy of cybercrime

Cybercrimes can be classified under different definitions and according to different standards. Scholars have proposed numerous plans for categorizing cybercrimes. For example, Bequai (1979, pp. 106-107), who originally

regarded cybercrime as part of white-collar crime, proposed to classify computer crime into five categories, including vandalism, theft of information, theft of services, theft of merchandize or other property, and fraud. Bequai (1983) thereafter developed his classification into seven categories, including financial thefts, frauds, and abuses; thefts of property; abuses of data; unauthorized use of services; vandalism; sabotage, and political and industrial espionage (pp. 17-21). Wasik (1991, pp. 41-60) proposed six categories of computer misuse, including unauthorized access, computer fraud, unauthorized removal of data or programmes, unauthorized use of computer time or facility, and destruction and damage. Wasik (1991, pp. 24-33) put forward three levels of relationships between the conceptions of computer crime and white-collar crime: (1) corporate crime, (2) occupational crime, and (3) misuse committed by outsiders. To a certain extent, this can also be regarded as a classification system. Grabosky (2000) considered nine varieties of cybercrime, including theft of services, communications in furtherance of criminal conspiracies, information piracy and forgery, the dissemination of offensive materials (including extortion threats), electronic money laundering; electronic vandalism and terrorism; telemarketing fraud, illegal interception, and electronic funds transfer fraud (pp. 3-8). Icove and co workers (1995), Sieber (1996), and many other scholars have also proposed various methods of classification. An exhaustive bibliography is neither necessary nor possible. However, this section will present a classification method according to the roles that data processing systems play in offences.

Many earlier definitions of computer crime have already contained some methods of classification based on the different roles of the computer in offences. The development process is from simple categories to complex categories. The earliest definition contained the only category, that is, crime by computer (for example Parker 1976). A subsequent definition contained two categories, that is, crime by computer and crime against the computer.[1] MacKinnon (1997) classified cybercrime into computer-incidental crimes and

[1] In the network environment, scholars have also transplanted this category in their research on cybercrime. Casey (2000), as cited in Levinson (2002), p. 455, saying that cybercrime can be a traditional crime that is committed through the use of a computer or the Internet, or a crime that involves particularly the targeting of computer technology.

computer-instrumental crimes, and defined computer-incidental crimes as offences in which the computers are merely used "incidentally or tangentially"; computer-instrumental crimes involve computers more "directly" as the "tool" or instrument (MacKinnon 1997, p. 210). The U. S. Department of Justice (2000) categorized computer crime into crimes in which computers are targets, storage devices, and communications tools. Parker and Nycum (1984, pp. 313-314) identified four ways of committing criminal acts with computers, that is, the computer as the object, subject, tool of the crime, and the symbol of the computer used in intimidation or deception. Carter (1995) divided computer crimes into four categories, including offences in which the computer was the target; the computer was the instrument of the crime; the computer was incidental to other crimes; and crimes associated with the prevalence of computers. Whereas data processing systems play an increasingly essential role in contemporary society, considering that the offences accompanied by data processing systems are being increasingly diversified, we feel that there is a need to expand the categories of cybercrime with regard to data processing systems. In discussing digital extortion, Grabosky (2000) has listed the roles of data processing systems as media for threat, targets of threatened action, media for disclosure of embarrassing personal details, means of facilitating payment, and incidental to the offence (pp. 34-50). All these discussions prove that data processing systems can play a variety of roles in offences.

In the following sections, I will expand the roles of data processing systems in cybercrime and divide cybercrime into seven categories. Data processing systems can be mass media, operating mechanism, place of occurrence, transfer channel, targeted object, and multiple-purpose instrument, or used in the preparation for other crimes. In previous literature, the dichotomy recognized the roles of data processing systems used to be summarized as target and tool (or termed instrumentality). The term "tool" or "instrumentality" has been used in an unlimited broad way. In practice, the roles that data processing systems can play are far more abundant than merely being a tool or an instrumentality.

Data processing systems as a targeted object of the offence

"Computers are targets" is a subtitle in Bequai (1983, pp. 7-11). At present, we can roughly assert that the whole data processing systems are targets. In a certain sense, data processing systems can be regarded as networked assets (Wells and Sevilla 2003), including tangible assets and intangible assets, hardware and software, intra-national assets and international assets. Networked assets are a kind of combinative assets existing in cyberspace. Furthermore, networked assets are dynamic, existing in the process of production, which constitutes a kind of production management, for example, covering activities that can be included in the field of electronic commerce.

The economy, national security, politics, military affairs, science and technology, education and medicine increasingly depend on the Internet, through which information is created, stored, transmitted and processed. When information security is threatened, the whole country will suffer great losses.

The Internet is vulnerable to artificial attacks, some of which belong to traditional crimes, for example, cutting off the electricity supply, destroying cables, moving antennae used in satellite communications; and more traditional crimes, for example, destruction of computers and peripheral facilities.[2] Nowadays, these actions are not uniformly regarded as cybercrime. Cybercrime against the Internet mainly exploits computer technology. The most typical attacks are through computer viruses and other malicious programmes. There has already been a long list of instances of serious viruses.

In fact, sometimes computers and networks have the nature of both instrument and target. For example, an attack on the Internet must be launched through the Internet itself. As mentioned above, these classifications are not mutually exclusive. Rather, they can be carried out in a compatible way. The perpetrator's Internet resources are more likely to be used as instruments, while that of the others are more likely to be aimed at as targets. The Internet is, however, composed of huge indivisible systems that can be both exploited

[2] These were regarded as computer crimes in books published several years ago. For example, Icove and co-workers (1995), saying that "Terrorist bombings on buildings housing computer equipment, arson, and theft and destruction of computer equipment fall into this category."

or attacked.

It should also be emphasized that, "the stealing of computers, computer chips and other computer equipments from commercial premises" as in R. v. Kehoe and Others,[3] might seem not so relevant to our discussion at first glance. However, a natural result of these activities is that a computer-aided business and computer-processed data may be damaged, and thus it remains a cybercrime in our sense. Taking into account the disabling of the functioning of whole data processing systems, and the loss of information in internal memory media, thefts of computers and their parts represent more than illegal access to the systems and information. For instance, in Investigation into Security of Personal Information Held by Vancouver Coastal Health Authority's Employee and Family Assistance Programme, the thief stole from the office of manager of the administration a desktop computer containing a database of approximately 11,000 clients.[4]

A different situation appeared in R. v. Moseley,[5] where the victim was robbed of property, including "computer and electrical equipment, a rucksack and a personal organiser, and cash cards." In THO:2005:28, two portable computers were found at the accused's two residences. The charge and the conviction against the perpetrator mentioned nothing about the particularity of the computer and the information inside it. The computer here is nothing more than a target of traditional robbery—no data processing systems were interrupted, and no information was destroyed or disclosed.

In addition, the term data processing systems is used here in a broad sense as referring to data processing systems and the information in them. In practice, these two conceptions are usually used separately. For example, in the U. K., the Computer Misuse Act 1990 has been assigned the principal function of defending the integrity of the systems but not of information, while the latter

---

[3] It has been dubbed a "highly sophisticated and successful criminal enterprise," what one of the perpetrators confessed as that "Computer crime is what I do." [1998] EWCA Crim 1163 (1st April, 1998). See also Section 6.3.

[4] Investigation into Security of Personal Information Held by Vancouver Coastal Health Authority's Employee and Family Assistance Program, Re, 2006 CanLII 20511 (BC I.P.C.).

[5] [1999] EWCA Crim 1089 (21st April, 1999).

task falls on the Data Protection Act 1984.[6]

Offences in which data processing systems are targeted roughly cover:

1. Unauthorized access to data processing systems,[7]

2. Unauthorized access to information,[8]

3. Unauthorized alteration of information,[9]

4. Unauthorized interruption of data processing systems,[10]

5. Attack by viruses, worms, logic bomb, Trojan horse, and other malicious

---

[6] DPP v. Bignall [1997] EWHC Admin 476 (16 May 1997)

[7] This has been criminalized by Convention on Cybercrime, Article 2; the Danish Penal Code Article 263, Section 2; the Finnish Penal Code Article 28; the Swedish Penal Code, Chapter 4, Section 9c. In United States v. Sablan (Ninth Circuit No. 94-10533, D. C. No. CR-94-00017-JSU, 7 August 1996), the accused has recently been dismissed from a bank. After some drinking, she used a key she had kept and went to her former work site, where she used an old password to log into the bank's computer, modified or deleted several files, and then logged off.

[8] In legal instruments, illegal access to information system and illegal access to the information in the system are usually linked together, neglecting their obvious difference. In the Convention on Cybercrime, Article 2, illegal access to information was the purpose of illegal access to an information system. A similar provision is seen in the Danish Penal Code Article 263, Section 2. the Finnish Penal Code distinguishes between these two acts, dealing with illegal access to information in Article 38. See also the Swedish Penal Code, Chapter 4, Section 9a. In United States v. Czubinski (First Circuit No. 96-1317, 21 February 1997), the court reversed the original conviction, which was based on the accused's "unauthorized browsing of taxpayer files" with his valid password, even though he was required to access only accounts needed to accomplish his official duties.

[9] Convention on Cybercrime, Article 4, providing computer-related fraud through inputting, altering, deleting or suppressing computer data, interfering with the functioning of the computer system. It covers both alteration of information and influence on the information system. See also the Danish Penal Code, Article 291; the Finnish Penal Code, Articles 33 and 35; the Swedish Penal Code, Chapter 12, and when the acts involve public danger, Chapter 13, Sections 4 and 5. In United States v. Magnuson (Fourth Circuit No. 964957, D. C. No. CR-96-186-A, 24 June 1997), the accused used his home computer to intrude into and disable the victim's computer servers in seven states.

[10] Convention on Cybercrime, Article 5. See also the Danish Penal Code, Article 193; the Finnish Penal Code, Article 35; the Swedish Penal Code, Chapter 12, and when the acts involve public danger, Chapter 13, Section 4 and 5.

programmes,[11]

6. Theft of computer time, network time, or telecommunications services, a specific form of illegal access,

7. Possession, disclosure and providing unauthorized persons with unauthorized information; or unauthorized possession, disclosure and providing unauthorized persons with information, both being the extension of illegal access to information.[12]

8. Unauthorized interception of communications.[13]

Data processing systems as multi-purpose instrument of the offence

The offences in which computers and networks are utilized as tools have the longest history in computer crime (Parker 1976; Bequai 1978). Networks are widely interconnected outside the limits of time and the boundary of space. As society is becoming more dependent upon computer data processing and the telecommunications systems. With the Internet, crackers intrude into others' computers, web sites, e-mail accounts of individual and organizational users whose data, secrets, privacy and electronic property are stored there.

Under these circumstances, the Internet is becoming the instrument by which

---

[11] Convention on Cybercrime, Article 6. See also Danish Penal Code, Articles 193 and 291; Finnish Penal Code, Articles 33 and 35; Swedish Penal Code, Chapter 12, and when the acts involve public danger, Chapter 13, Sections 4 and 5. In United States v. Sullivan, (Fourth Circuit No. 01-4330, 25 January 2002), the perpetrator planted a logic bomb into the software prepared for the company before he quit. Four months later, the logic bomb disabled hundreds of hand-held computers used by the company's sales representatives to communicate with headquarters.

[12] In the United Sates v. Pitts (Fourth Circuit No. 97-4616, 28 January 1999), the accused, who "was trusted with access to very sensitive and highly classified materials related to counterintelligence operations, surveillance of Soviet officials assigned to the United Nations, and the true identities of American agents and Soviet defectors", "attempted to provide or made preparations to provide his undercover FBI handlers with computer diskettes containing information classified as 'Secret'..."

[13] Convention on Cybercrime, Article 3. See also the Danish Penal Code, Article 263; the Finnish Penal Code, Article 38; the Swedish Penal Code, Chapter 4, Section 8.

perpetrators commit not only traditional crimes but also new crimes. It is not only the instrument by which people commit crimes, but also the instrument through which people are victimized. In using the Internet, some people unwittingly break the law, while others are unwittingly harmed by crimes. Definitely, under more circumstances, perpetrators intentionally use the Internet to commit criminal acts. Therefore, the crackers who intrude into others' cyberspace through wired or wireless connections to the Internet are violating others' privacy, plundering others' data, stealing others' secret information, and embezzling others' property.

This kind of cyber instrument contains both the similarities and the differences from the traditional instruments. The case where one opens others' e-mails by a password, then marks it as unread and exits, is comparable to the case where someone opens one of the letters of another with a knife, and then seals it with glue. They both constitute an infringement of freedom of correspondence, but the concept of instrumentality is different. The instrument of the Internet bears with it the characteristic of a remote control, in which the criminal is not necessarily present in person at the crime scene where the letters exist, and does not necessarily leave footprints or fingerprints. The traditional notion of crime scene also changes because of this instrument.

Offences in which data processing systems are used as instruments roughly cover:

1. Forgery and counterfeiting,[14]

[14] The Convention on Cybercrime specifies the criminalization of computer-related forgery, as an act committed through inputting, altering, deleting, or suppressing data. In the national domain, these crimes induce no obstacle to applying traditional law, for example, the Finnish Penal Code, Article 33 can be applied to computer-related forgery. For example, in R. v. Lloyd ([1996] EWCA Crim 1744 (17 December 1996)), the accused was found using a computer with programmes for manufacturing compact discs , a compact writer and blank compact discs to replicate computer programmes. In R. v. Boutrab ([2005] NICC 36 (24 November 2005)), the accused used a false passport with the intent of inducing an employee to accept it. In R. v. Adeoye & Anor ([1997] EWCA Crim 1343 (3 June 1997)), the perpetrator used computer programmes to produce credit cards from plastic blanks. In search, "the police found a printout containing 10,000 credit-card numbers produced by a computer programme." In RovHO

2. Computer-aided unauthorized copy of software and other copyrighted works,[15]

3. Telecommunication piracy,[16]

4. Fraud using data processing systems,[17]

5. Password sniffering and keylogging.[18]

Data processing systems as mass media for the offence

As a form of media, computer networks have their advantages over the

12.06.2001 335, the three suspects, with the assistance of the computer, forged identity cards used for the unauthorized users to watch television programmes transmitted by a company.

[15] See for example, R. v. Johnstone ([2003] UKHL 28 (22 May 2003)), in which the accused pirated recordings and made compact discs and audio cassettes. In THO:2006:6, the accused was said to have made, without the permission of the right holder, 381 karaoke CDs in order to make a profit through using them in the karaoke business. In KouHO:2005:11, the co-defendants cooperated to make and sell DVD copies without the permission of the right holders.

[16] In United States v. Clayton (Ninth Circuit No. 96-10127, 11 March 1997), "cloning" was practised by the perpetrator to replicate the stolen identification numbers of legal mobile phones with the help of computer software; they were then used to make calls at the expense of the owner of the legal phone. See also United States v. Cabrera (Eleventh Circuit Nos. 98-4432, 98-4434, D .C. Nos. 96-CR-562-DLG, 98-CR-77-DLG, 19 April 1999), where the accused used a small device named “copy-cat” to clone cellular phone.

[17] In R. v. Russell ([2001] NICA 45 (12 October 2001)), the accused used a computer identification number and password to access confidential files in the computer system, identifying persons that he considered likely to claim any type of benefit, and gathering names, addresses and national insurance numbers. After this, he passed the information to a co-offender to make false claims for fraudulent benefits. In R. v. Farkas (2006 ONCJ 121, 10 April 2006), the accused made a profit of 45,000 dollars from victims in the U. S., Canada, and England through fraudulently acquiring goods and fraudulently selling them over a period of 18 months via the Internet purchasing and auction. During the fraud, he obtained credit-card information through on-line chat groups and bulletin-board systems. He sold these goods to legal collectors, during which he received money but did not send the goods to the purchasers.

[18] In United States v. Ropp (C. D. California, 7 October 2004), the accused placed a keylogging device on the cable that connected the victim’s keyboard to her computer's central processing unit, recording and storing what the victim typed with the keyboard. The indictment was dismissed, but the court made it clear how keylogging works.

traditional mass media. They surpass the limits of time and space, languages and traffic, and political and legal boundaries. The Internet enables people to "upload, post, e-mail, transmit or otherwise make available content that is unlawful, harmful, threatening, abusive, harassing, tortuous, defamatory, vulgar, obscene, libellous, invasive of another's privacy, hateful, or racially, ethnically or otherwise objectionable."[19] In fact, racist speech, tutorials for killing, raping, arson, bomb-making and even instructions for virus creating, malicious programme writing, and other forms of cyber attacks are widespread on the Internet. Various degree of political incitement, libel, rumour and superstition crowd up to mislead the public, going even further than the traditional media. Many countries are confronted with web sites managed by separatists, dissidents, and international opposition forces. These web sites always publish their opinions that are harmful to their government but beneficial to themselves. Now, information of this kind is being practically exported and imported across national borders at the speed of light.

One of the notable problems is slander, the false statements that come across the innovative online media injuring others' reputations by publishing false statements. The forms of such slander mainly include impersonating others to solicit sex mates, one-night lovers, publicizing others' telephone numbers, and fabricating photos by inserting the photos of other persons into pornographic photos, etc.

In addition, the online content may cause an international concern, such as racist and xenophobic material, that is, "any written material, any image or any other representation of ideas or theories, which advocates, promotes or incites hatred, discrimination or violence, against any individual or group of individuals, based on race, colour, descent or national or ethnic origin, as well as religion if used as a pretext for any of these factors."[20]

Offences in which data processing systems act as mass media roughly cover:

---

[19] See Yahoo! Terms of Service. Retrieved 5 May 2016, from http://docs.yahoo.com/info/terms/

[20] Additional Protocol to the Convention on Cybercrime Concerning the Criminalization of Acts of a Racist and Xenophobia Nature Committed through Computer Systems, Strasbourg, 7 November 2002, Article 2.

1. Dissemination of obscene material, in particular child pornography,[21]

2. Dissemination of racist and xenophobic material through computer systems,[22]

3. Online false statement about individuals or corporations,[23]

4. Indecent exposure,[24]

---

[21] In United States v. Slanina (First Circuit, No. 00-20926, 12 February 2002), the accused was convicted of using a city computer to access newsgroups and download pictures of child pornography. In R. v. Kozun (2007 MBPC 7), the accused distributed child pornography through his own personal computer, in which a programme converted the computer into an automated trading centre on the networks. The police found 3522 files (3368 pictures and 154 movies) in his computer that could be considered as child pornography and available for trade. The age-range of the children involved was between 8 months and 14 years. In Alan Joseph Ogilvie v. Her Majesty's Advocate [2001] ScotHC 69 (27th July, 2001), the accused downloaded from the Internet 12,000 images of child pornography onto his first computer and upon its confiscation, he downloaded a further 10,000 images of the same nature into his newly-bought second computer. In the Convention on Cybercrime, Article 9 criminalizes offences related to child pornography.

[22] In the Additional Protocol to the Convention on Cybercrime, Concerning the Criminalization of Acts of a Racist and Xenophobic Nature Committed through Computer Systems (2003), Article 3 criminalizes dissemination of racist and xenophobic material through computer systems, Article 4 criminalizes racist and xenophobic motivated threat, Article 5 criminalizes racist and xenophobic motivated insult, Article 6 criminalizes denial, gross minimization, approval or justification of genocide or crimes against humanity, and Article 7 criminalizes aiding and abetting.

[23] Defamation, including libel and slander, can be dealt with either civilly or criminally, in different jurisdictions. In the U. K., many cases have been settled in civil actions, for example, Godfrey v. Demon Internet Limited [1999] EWHC QB 244 (26th March, 1999) , where the accused party hosting a newsgroup in the U. S. published a piece that was "squalid, obscene and defamatory of" the victim; Robertson v. Newquest (Sunday Herald) Ltd & Ors [2006] ScotCS CSOH_97 (28 June 2006), where the defendant, a newspaper, which had an online edition, in which a notice was considered of a defamatory nature by the plaintiff was posted by a member of public; in Turner v News Group Newspapers Ltd. & Anor [2005] EWHC 892 (QB) (12 May 2005), the co-defendants, including one of the victim's former wives and a newspaper published an article on how the victim pursued sex with strangers in both printed and online forms.

[24] In Robertson v. Her Majesty's Advocate ([2004] ScotHC 11 (17 February 2004)), the perpetrator induced a seven year old girl to dance naked in front of a webcam and lick her private parts in front of said webcam, *inter alia* (paragraph 9).

5. False advertising,

6. Disclosure of confidential information.[25]

Data processing systems as a transfer channel to the offence

Cybercriminals can launch attacks from any computer in different jurisdictions. The continued development of techniques and skills for attacks makes it more difficult and complicated to investigate and prosecute these crimes (McConnell International 2000, pp. 1-2). Data processing systems can be used to transmit various malicious programmes that have the capacity to disrupt, destroy or limit the functions of data processing systems. For crackers, using software tools installed on a computer in a remote location, can illegally access to computer systems to obtain data, plant viruses or Trojan horses, or cause less serious mischief by changing user names or passwords. As to spies, corporations and governments are committing espionage through the superhighway of the world's Internet (Li 2009b). Espionage can penetrate the best security systems and the highest levels of management in cyberspace. Pirates, in their turn, can perfectly reproduce and easily disseminate text, audio, video or multimedia works by using digital technology (Grabosky 2000, p. 8). Some web sites are devoted to "charities" of this kind, similar to providing relief for the poor, who cannot afford expensive software, and thus the market of piracy acts as a solution to satisfy these users. The Internet has increasingly been exploited to distribute pirated works, with the development of new file-sharing techniques.

In the case of illegal access to others' web sites, the intruders may view no document, but usually view encrypted or unencrypted documents, obtain documents, read or delete e-mails, reveal documents to others, destroy files

[25] In Edward Yearly v. Crown Prosecution Service ([1997] EWHC Admin 308 21 March 1997), the perpetrator published confidential information that he obtained by unauthorized access. There have been numerous cases of such a nature in recent years in the U.K., for example, Grimm (2005, p. 598) reported that 140 applications for the National Institutes of Health (NIH) grant had been leaked on to open access web pages.

and make the systems inoperable, or use others' accounts to connect with the Internet. The attacks on web sites are growing in intensity. In the end 1990s and early 2000s, for example, according to the data of the previous Alldas web site, forty-seven attackers defaced 72 web sites in 1998, about 430 attackers defaced 1,079 web sites in 1999, about 2,555 attackers defaced 4,394 web sites in 2000, and in the first quarter of 2001, about 667 attackers defaced 4,797 web sites, a number greater than the victimized web sites of the previous year. Among these cases, the first 15 attackers who defaced at least one percent of the defaced web sites, did one-third of the defacement. The first eight top domain names of the mostly defaced web sites were: ".com," ".br", ".net", ".cn", ".tw", ".org", ".edu", and ".us".[26] Although the similar source is at present unavailable and several years has passed, this old information indicates that the web sites in the Asian Pacific region rather than Europe are the most likely to be defaced.

The computer systems of national defence of various countries are also the primary targets for hackers. In some cases, the passwords of these agencies were successfully cracked, and other secret information was obtained and disclosed.

Offences in which data processing systems act as a transfer channel roughly cover:

1. E-mail bombing,[27]

2. Harassment through electronic communication,[28]

---

[26] These data are obtained and calculated from http://alldas.de by the author in 2001. Later the web site became unavailable.

[27] For an explanation of e-mail bombing and other e-mail related crimes, see Planet India Website, E-mail Related Crimes, n. d. Retrieved 5 May 2016, from http://cybercrime.planetindia.net/email_crimes.htm. There, the E-mail bombing is defined as "sending a large amount of emails to the victim resulting in the victim's email account (in case of an individual) or servers (in case of a company or an email service provider) crashing."

[28] See, for example, R. v. Jonhson (Johnson, R (on the application of) v DPP [2005] EWHC 3123 (Admin) (8 December 2005)), the accused used both traditional mail and electronic means to harass the victim. He searched the home address of the victim through the Internet, and sent

3. Identity theft and cyberstalking (Li 2009a),

4. Denial of service attacks (cyber terrorism),

5. Distribution of pirated software, books, magazines, audio, video or live performances, etc.,[29]

6. Infringement of industrial secrets and state secrets,

7. Transmission of child pornography.[30]

Data processing systems as a place of occurrence of the offence

In the information age, much of the money, assets, state secrets and personal privacy are transformed into computer data and stored in computers, or circulated through the Internet. Meanwhile, networks become a giant gallery

letters or e-mails, harassing the victim directly, or sent letters or e-mails to the employer of the victim questioning her conduct, harassing her indirectly. This behaviour not only affected the victim herself, but also her family and others. In R. v. Debnath ([2005] EWCA Crim 3472), the female perpetrator harassed the male victim by sending fake e-mails to his fiancée and employer; by registering the victim on a web site for people with sexually transmitted diseases seeking sexual liaisons; and by setting up a web site, which had fake information detailing alleged homosexual practices by the victim, and so forth. In X v. European Central Bank ((Officials) [2001] EUECJ T-333/99 (18 October 2001)), the perpetrator repeatedly procured through the Internet documents of a pornographic and political nature and, of having sent them to third parties through e-mails, sent his colleague numerous messages through e-mails containing pornographic and ideologically extreme materials, despite the disapproval of the colleague concerned.

[29] In KKO:1999:115, the accused allowed e-mail users to copy computer programmes from the mailbox. The mailbox could be viewed as a deposit place, but the software was transferred through information systems.

[30] In United States v. Muick (Seventh Circuit No. 97-CR-30004, 8 February 1999), the American defendant used telephone and modem to download child pornography from a computer in Mexico in 1994, when the Internet was not pervasive. In R. v. Treleaven (Provincial Court of Alberta, 2006 ABPC 99, No. 060138286P1, 24 April 2006), the accused possessed 20 gigabytes of child pornography files which were identified depicted real children of both genders. While the police arrested him, his computer was still online, with dozens of other users queuing up to access the pornography.

of pornography, or a gambling house. Networks do not have value orientation, have no culture, have no legal consciousness, but the information stored and the activities taking place are either protected or prohibited by law. Furthermore, the "place" of networks is trans-territorial outside a unified legal system. Aggressions and harm take place at the terminals, which seems to be the only place where the crimes occur.

Factually, this is contradictory brought about by the special characteristic of the "place" of network. When the Internet is used to facilitate gambling, pornography, prostitution or trading in prohibited drugs, it become a cyber casino, a cyber brothel, a cyber museum or a cyber storehouse.

Definitely, the Internet cannot be a real place for prostitution, but it facilitates the provision of and spread of information about prostitution to unspecified third parties. The Internet can also be a convenient marketplace for pirated software, books, pictures and audio discs and videodiscs. People also transact prohibited articles as well as prescribed medicine, including weapons, drugs, and philtres. Advertisements for the transaction of human organs also appear on the Internet (Li 2003).

In some countries, it is prohibited to create, replicate and spread pornography, either adult or child, either online or offline. In addition, downloading and browsing pornographic web pages is illegal as well. In some other countries, however, adult pornography is legal. The conflict of jurisdiction may also take place in gambling and prostitution, drug trafficking, money laundering, and trade in weapons and even human trafficking. It is beyond the reach of domestic laws. More than ever before, the conflicts of criminal jurisdictions have become a serious concern. Thus in the face of the Internet, state control is diminished and criminals can launch attacks from another country where law enforcement is absent.

Furthermore, the Internet is likely to become the battlefield where cyber warfare takes place. The cyber-war criminals should be held liable for offences comparable to those punished by present international criminal law (however, for an analysis of cyber warfare, see Li 2010).

Offences in which data processing systems appear as crime scenes roughly

cover:

1. Intellectual property infringement,[31]

2. Collection and exhibition of child pornography,[32]

3. Sale of illegal articles (such as fire arms, alcohol, prescriptive drugs and other controlled substances),[33]

4. Online (illegal) gambling,

5. Fraud on the Internet (such as Internet auction fraud, multi-level marketing fraud).

Data processing systems as operating mechanism of the offence

Computers and networks can also be a means in offences such as assault, threat, harassment, creating a false alarm, spam and fraud through text, audio or video information (for detailed research, refer to Li 2005a; Li 2005b; Li 2006; Li 2007a). Data processing systems are used as a means of communications in these cases. The comparable traditional mechanism is the postal system and telephone system. Dissidents have found ways of using e-

[31] Convention on Cybercrime, Article 10 criminalizes offences related to infringements of copyright and related rights.

[32] The hard drive and other deposit media can easily save thousands of images. In R. v. Paton (2005 NUCJ 7), the accused saved approximately two thousand images of children in the hard drive of his computer. In United States v. Long (Seventh Circuit No. 04-1721, 22 February 2005), the accused saved tens of thousands of images of child pornography on a computer that he kept at work (p. 1); while in the United Stated v. Newson (Seventh Circuit No. 03-3366, 5 April 2004), the perpetrator saved child pornography (pictures of his daughter and his ex-girlfriend's daughter) in his own computer. In R. v. Reynolds & Ors ([2007] EWCA Crim 538 (08 March 2007)), the police found in the computer equipment a total of "1,757 still photographs and eight movies at level 1; 1404 stills and 46 movies at level 2; 54 stills and 2 movies at level 3; 22 stills and one movie at level 4; and 7 stills at level 5."

[33] For example, in R. v. Hamilton, 2005 SCC 47, Docket: 30021, over the Internet the accused sold a package of 200 files, about 5 of which "contained material relating to constructing bombs, breaking and entering, and 'visa hacking'," one of which "contained information on a credit-card number generator" (paragraph 2).

mail and WWW as both media and means to air effectively their political grievances. As to data processing systems as a means, the e-mail and WWW simply play the function of a post office or a telephone company. Information can be exported from one part of the globe, where it is not necessarily illegal, to a state where possession of such data is criminalized. The e-mail and WWW also provide dissidents with an uncontrollable means of communication between their domestic and overseas comrades. This has implications for the freedom speech of citizens and the state stability of related countries.

Offences in which data processing systems act as operating mechanism roughly cover:

1. Electronic extortion, harassment, creating a false alarm, threatening, and assault,[34]

2. E-mail spoofing (phishing).[35]

---

[34] In United States v. Ray (Eighth Circuit, No. 05-1655, 15 November 2005), the perpetrator sent e-mails to a company to extort 2.5 million US dollars by threatening to exploiting a breach in its computer security (p. 1). In R. v. Lefave (Ontorio Supreme Court of Justice Court File No. CrimJ(P)6527/02, 3 October 2003), during an Internet chat between a woman and a man, the man who later became the accused stated that he "wanted to rape his seven year old daughter and kill himself." The woman disclosed the concerns to the police. He was charged with communicating a threat using a computer.

[35] Phishing "consists of creating fictitious domain names and websites all with a view to extracting bank account details from gullible individuals." See Novus Credit Services Inc v Discover Financial Services LL C [2006] DRS 03205 (27 January 2006). Through phishing site, the perpetrator can obtain "key personal details from users of the webpages to which those domain names resolved" "fraudulently" (See Alliance & Leicester PLC v Brawn [2006] DRS 4135 (18 December 2006)) or the perpetrator may acquire "confidential financial information inappropriately" (See Royal Bank of Scotland Group PLC v Laverio [2006] DRS 3953 (16 October 2006)). In United States v. Desir (Western District of Pennsylvania, 2005), the accused devised a scheme to defraud through fraudulent web sites, persons who believed they were dealing with web sites of legitimate institutions, and online auction and payment services. E-mail spoofing can also be used in e-mail bombing. For example, in United States v. Carlson (Third Circuit No. 05-3562, 12 December 2006), the accused launched two types of e-mail attacks: direct attack, in which he directly sent thousands of e-mails from different addresses to one address to flood it; and indirect attack, in which he sent one e-mail from one address to thousands of different addresses, but the sending address was the one that he spoofed.

Data processing systems used in preparation for other offences

Data processing systems are increasingly being used to prepare for further offences. These offences include both cybercrimes and traditional offences. More and more traditional offences against person or property seek assistance from data processing systems. Wasik (1991) stated that "it is certainly conceivable that a computer may be used as the means of bringing about a person's death or causing physical injury," with associated offences including destruction and damage, denial of access to authorized users, death, physical injury, and endangerment, blackmail, corruption, official secrets, etc. (p. 150) Perpetrators frequently exploit data processing systems in two ways. One is that perpetrators conspire through the Internet (for example Guo and Wang, Great River Newspaper, 29 July 2003). Other cases have also involved conspiracy to commit robbery, abduction, and so forth. The second manner of exploitation is that the perpetrators pursue victims through the Internet. The most common cases involve robbery, abduction, murder, blackmail, and rape (for example, Geng, Pingliang Daily, 27 February 2003).

Cybercrime is a topic covering a very wide scope. Almost all the traditional crimes, including murder and arson, can be committed with the assistance of computers and networks. To call these crimes cybercrime is not inappropriate, and consideration of the use of computers and networks into research of these crimes is also necessary.

However, this article studies cybercrimes with unique characteristics, specifically, the crimes relating to security, including the security of data processing systems, the security of e-commerce, and the security in which data processing systems serve a critical infrastructure. Although murder and arson are also tied up the issue of security, for example, the security of life and health, public security, property security and so forth, they are neither unique to the information society nor do they have special features. The crimes discussed in this article are limited to those in which data processing systems play a unique role, as either target, tool, route, place, medium, means, or they are used in preparation for other crimes. Other crimes may be referred to when necessary in discussing these crimes.

Offences in which data processing systems are used in preparation for other crimes cover a broad range, but the most usual ones roughly cover:

1. Communications in furtherance of criminal activity or criminal conspiracy,[36]

2. Electronic money laundering,

3. Online tax evasion,

[36] In R. v. Poon and Wong, 2006 BCSC 1824, Docket: 23635, four offenders abducted a victim from whose family they requested a ransom, during which they sent proof-of-life photographs through the emails to the victim's family or friends (paragraph 15). In R. v. Kwok, 2007 CanLII 2942 (ON S.C.), Docket: P134/06, from the computer of the accused were revealed of about 2000 images and 60 video clips of child pornography. Along with these materials was recovered written material of "graphic chatroom conversations between paedophiles about how much they enjoy sexually abusing young children and babies and about where pictures and videos of such activity can be obtained." (paragraph 1). In R. v. O'Brien (2002 YKTC 94, Docket: 02-00176A • 02-00305), the accused used pagers, cell phones and computer internet email to communicate with cocaine suppliers and other associates(paragraph 4). In R. v. Brown, 2006 CanLII 12302 (ON S.C.), Docket: C44863, the accused used e-mail and other online communications to contact a girl on the age of 13, with the intent making her leave her family. In United States v. Christopher Lee Adjani; Jana Reinhold (No. 05-50092 D. C. No. CR-04-00199-TJH-01 OPINION, 13 January 2006), the accused were charged with conspiring to commit extortion and transmitting threatening communications with intent to extort, based partly on the incriminating e-mails seized in their computers (p. 7581). In R. v. Taylor and Burin ([1997] EWCA Crim 1074 (2 May 1997)), Burin made checks on the Police National Computer to obtain the address of the owner of a car (usually one he had recently sold to the new owner) and passed the information to Taylor to use it to steal the car. Burin also modified information so that stolen vehicles would appear to be recovered, enabling Taylor to possess stolen cars. In the U. K., Section 58(1) and (2) of the Terrorism Act 2000 provides that possession of a computer file of a particular nature is likely to be punished, even if it is freely downloaded from the Internet:

"(1) A person commits an offence if –

(a) he collects or makes a record of information of a kind likely to be useful to a person committing or preparing an act of terrorism, or

(b) he possesses a document or record containing information of that kind.

(2) In this section "record" includes a photographic or electronic record." Some cases have been punished according to this act, for example, R. v. Boutrab ([2005] NICC 36 (24 November 2005)).

4. E-mail spoofing (phishing).

5. Child exploitation.[37]

It is worth noting when I classify the potential roles of data processing systems in cybercrime or other crimes, I do not consider them as separate ones. As it has already been noted that, these roles can possibly be separated, found to be overlapping, or integrated in one and the same case. For instance, in McKinnon v USA & Anor,[38] the accused used his own computer to access illegally 97 computers of the U. S. government, installing remote control software, acquiring IDs and passwords, and deleting data from these computers. He even left a message expressing his interest in hacking these computers. Here, his own computer is a tool, the Internet is a route, and the U. S. governmental computers and the data in them are targets, and so forth. In R. v. DO,[39] the accused took the minor female victims to the computer and behaved indecently while chatting online with women, during which he also touched the victims inappropriately on the breasts and vagina, showing them online pornography.[40] The roles of data processing systems in such cases are multiple.

In drafting legislation, it is also hard to give a clear-cut division between the different roles of data processing systems or of the part of it relevant in detailed offences. If any efforts are to be made for determining such a borderline, for example, one of the most puzzling situations will be met with in an offence relating to cybercriminal devices, particularly unauthorized possession, transaction, transmission, and utilization of passwords.[41] The passwords can be regarded both as a target, being a part of data processing systems, and a tool, for illegal access to the other part of data processing systems, in the same offence.

---

[37] For example, in United States v. Meek (No. 03-10042, 12 January 2004), the accused used the instant messenger to lure a child into a sexual encounter.

[38] [2007] EWHC 762 (Admin) (03 April 2007).

[39] [2006] NICA 7 (10 March 2006).

[40] ibid., paragraph 9.

[41] Such conducts are criminalized in the Convention on Cybercrime as Misuse of Devices (Article 6).

Clarification of relevant conceptions

After reviewing previous definitions and providing a role-oriented definition, the current section will turn to clarify some relevant conceptions that are usually used to describe the characteristics of cybercrime. The definition of cybercrime has long been a pending question with regard to the existing criminological theories. The alternatives have been abundant and there have been a controversial exploiting of different theories by different researchers with different standpoints or with different empirical proofs. The concepts involved in this field include white-collar crime and economic crime, etc. The following paragraphs are designed to clarify the relationship between cybercrime and some of these concepts separately.

White-collar crime

Unlike most other criminal phenomena that bear traditional names, the conception of white-collar crime was coined by Edwin H. Sutherland in 1939[42] and defined "approximately as a crime committed by a person of respectability and high social status in the course of his occupation" (Sutherland 1949, p. 9). The historical development of and theoretical disputes over the patterns of white-collar crime have created many different definitions (Friedrichs 1996, pp. 2-11). Yet many are still making efforts to express their new understanding about the phenomenon (ibid., pp. 6-7; Helmkamp, Ball, and Townsend, 1996). The theories involved differ in emphasizing certain

[42] Geis and Goff stated in an introduction to the 1983 version of Sutherland's book "White-Collar Crime" that "The thirty-fourth annual meeting of the American Sociological Society – convened in Philadelphia in 1939 during the academic recess between Christmas and New Year- was held jointly with the fifty-second gathering of the American Economic Association…Sutherland's talk was entitled 'the While Collar Criminal,' and it altered the study of crime throughout the world in fundamental ways by focusing attention upon a form of lawbreaking that had previously been ignored by criminological scholars." (p. ix) Therefore, Sutherland initially coined the term "white-collar crime" in 1939, published the paper in 1940, and published the book in 1949.

characteristics of white-collar crime such as "commission in a legitimate occupational context, respectable social status of perpetrators, presence of calculation and rationality (with economic gain or occupational success a primary goal), absence of direct violence, offenders' noncriminal self-image, deterrence of and, a limited criminal justice system response." (Friedrichs 1996, p. 6, citing different sources) Debates among criminologists also extend to the terminology, definition, and other issues (ibid., pp. 6-7).

The proposal for a concept "white-collar crime" was prior to the invention of the computer and the establishment of computer networks in the present sense, and most certainly before the emergence of computer criminal phenomena. The involvement of data processing systems in white-collar criminal activities leads people to attribute computer crime to white-collar crime because the process of the former has usually been considered impossible without a high level of knowledge or without convenient opportunities for access to the machine. The general public used to view computer crime as complicated because they had little chance for revealing the truth of the digitalized processing. In addition, the reality of computer crime has possibly been distorted due to overemphasizing business victims and underemphasizing consumer victims (Kling 1980, p. 14).

Some studies have found that cybercrime is a low-technological crime, and not a high-tech crime (Molnar 1987). With the popular use of computers and networks, more than 17 percent of the world population are connected online (Internetworldstats.com 2007), and the growth rate is still high. The tools available to only a small group of computer users in the past are now available to a large population who have their own computers and who are connected to global networks. More and more potential cybercriminals do not need sophisticated skills for creating malicious codes by themselves. Compared with traditional violent crimes, a majority of current cybercriminals are not manufacturing guns and powder, but picking them up and shooting. Even the rest of the cybercriminals can use available programmes to produce malicious programmes to reach their goals. Therefore, "respectability and high social status" are irrelevant among today's cybercriminals.

Definitions of almost all derivatives have insisted that the offences involved are committed in the course of employment. In cybercrime, such offenders would express themselves in the form of launching inside attacks. But otherwise, I have found that insiders only make up one fifth of the cybercriminals successfully prosecuted (Li 2008). That is to say, most of these cybercriminals do not commit cybercrime in their employment. This provides further negative proofs against the claim that cybercrime is wholly coincident with the concept of white-collar crime.

Criminal phenomena, particularly those in new fields, are continuing to be transformed from simple to complex, from more traditional to more modern, from non-occupational to more occupational. White-collar criminals' increasing exploitation of data processing systems is a predictable tendency.

Economic crime

There has never been a widely accepted definition of economic crime. An example of one definition can be taken from Sjögren and Skogh (2004, p. 1), who have defined economic crime as a crime committed to gain profit within an otherwise legal business. Recommendation No. R (81) 12 of the Council of Europe's Committee of Ministers of 1981 listed a broad range of offences into economic crime, including computer crime, particularly theft of data, violation of secrets, and manipulation of computerized data. The relevant literature has taken it as natural that computer crime is a crime in which the computer is used as an instrument of economic crime (for example, Johnson 2006, p. 1). Actually, the motives of cybercrime can be very wide and cover dozens of different kinds of crime. Profit gaining is only one of the numerous motives of cybercrimes.

Although it is difficult to find a motive behind a cybercrime (Philip 2002, p. 7), many different studies and research have drawn diversified conclusions on the classification of motives. According to Jordan and Taylor (1998), there are six common attitudes among hackers: addiction, curiosity, thrill of information searches, ability to access, peer recognition, and identifying security loopholes. Maiwald (2003, pp. 36-38) has concluded that hacker

motivations fall into three categories, including the quest for challenge, greed, and malicious intent or vandalism. Kiger and co-workers (2004) have summarized the motivations of cybercrime as money, entertainment, ego, cause, entrance to social groups, and status. Pipkin (2002, pp. 17-28) has proposed that hackers may hack from a sense of intellectual motivation, such as educational experimentation, harmless fun, as a wake-up call; personally motivated, such as disgruntled employees, cyber-stalking; socially motivated, such as cyber-activism; politically motivated, such as cyber terrorism, cyber-warfare; financially motivated; and motivated by ego. Kremen (1998) has classified hackers into ten types with "different sizes, flavours and colours."

In fact, the motives of cybercrime may vary in a way that is beyond the imagination. If we say that many cybercriminals have similar motives, we can also say that nearly every perpetrator has his or her own. Bequai (1983, pp 44-45) has summarized 17 different kinds of motives that propel the potential perpetrators to take the risk of committing computer crime.

The reasonable conclusion drawn from the above studies is that the conceptions of cybercrime and economic crime are correlated but not identical. Some cybercrimes can be classified into economic crime, while some others cannot. It is also clear that economic crime committed with the computer and on computer networks make up only a part of the whole phenomenon of economic crime.

Corporate crime

Yeager and Clinard (2006) have defined corporate crime as "any act committed by corporations, that is punished by the state, regardless of whether it is punished under administrative, civil, or criminal law" (p. 16) and they have regarded it as a particular type of white-collar crime (p. 17). It is possible for corporations to commit cybercrime, and the relationships between these conceptions are become ever more puzzling.

What is still unclear is the extent to which computer crimes are committed by corporations. In Li (2008), corporate perpetrator was involved in only one out

of 115 cases, while all other cases were committed by either a single individual or group of individuals, at most the organized groups. Although the finding of the study cannot be regarded as having universality, it has sense in that not all cybercrime are being committed by corporations or organizations (Ibid).

Professional crime

Insiders and outsiders constitute different ratios in different categories of offences. The categories in which the insiders constitute the majority of offenders include: data theft, espionage, and fraud (Li 2008).

The categories in which outsiders constitute a majority of offenders include: all identity theft, 92.9 percent of embezzlement and corruption cases, 87 percent of attack and sabotage cases, 81.8 percent of viruses, worms, spyware and logic bombs, and 76.2 percent of hacking and sabotage cases. In fact, outsiders also constitute a strong ratio among fraudsters: about 42.9 percent (Ibid).

Former employees are included in the category of outsiders. A significant ratio of offenders who attack and sabotage are former employees, who constitute about 43.5 percent. Former employees also constitute 12.7 percent of offenders in hacking and illegal access cases, and about 7.2 percent of offenders in embezzlement and corruption cases (ibid).

Overall, insiders and outsiders constitute 21 percent and 79 percent of all reported offenders separately classified. Former employees constitute 16 percent of all the outsiders. If we add up former employees into insiders, they would constitute about 34 percent of the total number of offenders, still a smaller ratio than the outsiders. The safe conclusion is that cybercrime is again not a professional or occupational crime (ibid).

Trans-national crime

Globalization is the hallmark of modern economic and legal activities. The trans-border movement of personnel, goods, and information paints an embarrassing picture of national boundaries. Data processing systems alone are no longer subject to the physical limit of traditional countries. Many offences traditionally committed in neighbourhoods, communities, and native areas now extend beyond national boundaries. Many other offences traditionally committed in a trans-border manner are becoming a means to acquire new markets in the more networked globe. Some new offences can, indeed, only be completed in a trans-national style. Trans-national crime can be seen as the counterpart of international trade in civil society, being an involuntary transaction between perpetrators and the social order (in many cases, involving victims, but in many other cases, victimless).

For example, in McKinnon v USA & Anor,[43] the accused used his own computer in London and obtained unauthorized access to dozens of governmental computers of the U. S., from which he discovered the identities of certain administrative accounts and associated passwords. He installed remote control software on these administrative computers. The software enabled him to access and change data at any time.

Many people have taken it for granted that because computer networks are trans-national, naturally most crimes committed in relation to the networks are also trans-national. This poses a great concern among academia, law-enforcement agency, and legislature. However, this is still an unanswered question. In Li (2008), altogether 14 out of 115 cases were committed by international perpetrators or foreigners, a ratio weaker than 12.2 percent. Domestic perpetrators were responsible for the remaining 87.8 percent of cyber criminals. The majority of the reported cases are domestic computer offences (Ibid).

We can explain this phenomenon by listing the possibilities:

First, data processing systems have crossed the national boundaries, but prosecuted offences are mostly confined within these boundaries;

[43] [2007] EWHC 762 (Admin) (03 April 2007).

Second, due to lack of an international arrangement of law and enforcement, few trans-national cybercrime offenders have been investigated; and

Third, offences are mostly territory-dependent, and do not cross the border at all.

All these factors are responsible for the low likelihood of trans-national cybercrime, but, as we have seen and will see further, the absence of international legal harmonization and assistance mechanisms contributes primarily to the current invisibility of trans-national cybercrime (Li 2007b).

Conclusion

The phenomenon of cybercrime is comprised of complicated acts and facts, which are multifarious, concealed and changing. There is no ready-made theory applicable for defining and categorizing various practical cases. A great many disputes exist among experts as to what exactly constitutes a cybercrime, for there is a lack of an internationally recognized criterion. Due to the lack of unified definition and classification schedule, the co-existence of different viewpoints inevitably results in conflicts in international law enforcement and to a waste of judicial resources. Cybercrime includes both new crime utilizing computer systems and new forms of existing crimes exploiting computer systems.

Theoretical and legislative classifications group cybercrimes into different categories. However, the most characteristic pattern of cybercrime is that the detailed offences are more or less linked to data processing systems. The roles of data processing systems in the offences perpetrated have the potential to develop. The starting-point of cybercrime research should focus on the recognition of the roles of data processing systems in the offences perpetrated. It is the data processing system that makes perpetrators breach security protection, to exploit the function of this system, to transmit illegal materials through this system, to operate illegal commercial activities in this system, to air offensive speech in the forum of this system, to communicate with this system, and to use this system to prepare murder, harassment and other

traditional offences.

The definition does not determine the existence of cybercrime. Nevertheless, the definition endows this phenomenon a place on the academic terrain. Through definition, we are changing "cybercrime" into a research topic. Potential cyber warriors and cybercriminals may also learn from cybercrime incidences, about how they are committed, why they are reported, and what legal results are induced, etc., so that they can better trick the cybersecurity management, the victims and law-enforcement agencies. In contrast to the incentives of the crime perpetrators, scholars should analyse how and why these criminals are motivated and concealed (for the influence of anonymity, see Li 2014), how and why victims are exposed, and how and why guardianships are absent.

References

Bequai, A. 1978. *Computer Crime*, Lexington, Massachusetts, Toronto: Lexington Books.

Bequai, A. 1979. *White-Collar Crime: A 20th Century Crisis*, Lexington, Massachusetts: Lexington Books.

Bequai, A. 1983. *How to Prevent Computer Crime: A Guide for Managers*. New York, Chicago, Brisbane, Toronto, Singapore: John Wiley and Sons.

Brenner, S. W. 2001. Cybercrime Investigation and Prosecution: the Role of Penal and Procedural Law. Retrieved 5 May 2016, from http://unpan1.un.org/intradoc/groups/public/documents/APCITY/UNPAN003073.pdf

Carter, D. L. 1995. Computer Crime Categories, *Law Enforcement Bulletin*, U. S. Department of Justice: Federal Bureau of Investigation, volume 64, number 7, pp. 21-26.

Casey, E. 2000. *Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet*. London: Academic Press.

CCIPS. 2006. Computer Intrusion Cases. Retrieved 5 May 2016, from http://www.usdoj.gov/criminal/cybercrime/cccases.html

Commission of the European Communities. 2000. *Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-Related Crime,* COM (2000) 890 final.

Darlington, R. n.d. Crime on the Internet. Retrieved 5 May 2016, from http://www.rogerdarlington.co.uk/crimeonthenet.html

Dibbell, J. 1993. A Rape in Cyberspace, *Village Voice*, volume 38, number 51, pp. 36-42.

Friedrichs, D. 1996. Trusted Criminals-White-Collar Crime in Contemporary Society. Belmont, California: Wadsworth Publishing Company.

Goodman, M. D. 1997. Why the Police Don't Care About Computer Crime, *Harvard Journal of Law and Technology*, volume 10, number 3, pp. 465-494.

Gotterbarn, D. 1990. Computer Ethics: Responsibility Regained, *National Forum: The Phi Kappa Phi Journal*, volume 71, number 3, pp. 26-31. Reprinted in D. G. Johnson and H. Hissenbarn (ed.). *Computer Ethics and Social Value*, Englewood Cliffs, New Jersey: Prentice Hall, 1995, pp. 18-24.

Grabosky, P. 2000. Cyber Crime and Information Warfare, The Transnational Crime Conference convened by the Australian Institute of Criminology in association with the Australian Federal Police and Australian Customs Service and held in Canberra, 9-10 March. Retrieved 5 May 2016, from http://www.aic.gov.au/conferences/transnational/grabosky.pdf

Helmkamp, J.; Ball, R.; Townsend, K. 1996. Proceedings of the Academic Workshop: “Definitional Dilemma: Can and Should There Be a Universal Definition of White-collar crime?” Morgantown, West Virginia: National White-collar crime Centre.

Icove, D., and co-workers. 1995. Computer Crime: A Crimefighter's Handbook, O'Reilly and Associates.

Internetworldstats.com. 2007. Internet Usage Statistics-The Big Picture. Retrieved 27 July 2007, from http://www.internetworldstats.com/stats.htm.

Johnson, D. G. 1985. *Computer Ethics*, Englewood Cliffs: New Jersey: Prentice Hall.

Johnson, T. A. 2006. *Forensic Computer Crime Investigation*, Boca Raton, Florida: Taylor and Francis Group.

Jordan, T.; Taylor, P. A. 1998. Sociology of Hackers, *Sociological Review*, volume 46 number 4, pp. 757-81.

Kiger, M.; Arkin, O.; Stutzman, J. 2004. *Profiling. In The Honeynet Project Know Your Enemy: Learning about Security Threats*, Addison Wesley.

Kling, B. 1980. Computer Abuse and Computer Crime as Organizational Activities, *Computer/Law Journal*, vol. II, no. 2, pp. 12-24.

Kremen, S. H. 1998. Apprehending the Computer Hacker: The Collection and Use of Evidence, *Computer Forensics Online.* Retrieved 5 May 2016, from http://www.shk-dplc.com/cfo/articles/hack.htm

Levinson, D. (ed.). 2002. *Encyclopedia of Crime and Punishment*, Newbury Park, CA: Sage Publications.

Li, X. 1992. Lun Jusuanji Fanzui Xingfa Shiyong Wenti (Concerning the Application of Penal Law to Computer Crime), Graduate Law Review, *China University of Political Science and Law*, number 2.

Li, X. 1993. Jisuanji Fanzui Ruogan Wenti zhi Yanjiu (*A Study on Several Issues of Computer Crime)*, degree thesis for Master of Laws, China University of Political Science and Law.

Li, X. 2003. Lun Wangluo Fanzui (Crimes on the Internet), *Law Library*. Retrieved 5 May 2016, from http://www.law-lib.net/lw

Li, X. 2005a. Spam Solutions: A Law and Economics View. Asian and Comparative Law, vol. 3, no. 1, pp. 54−64.

Li, X. 2005b. Spam solutions: a law and economics view. International conference on law and economics and related topics, Helsinki, Finland.

Li, X. 2006. E-marketing, Unsolicited Commercial E-mail, and Legal Solutions. *Webology*, vol. 3, no. 1, pp. 1−15.

Li, X. 2007a. The Phenomenon of Unsolicited E-mails with Attachments. *SIMILE: Studies In Media & Information Literacy Education*, vol. 7, no. 2, pp. 1−11.

Li, X. 2007b. International Actions against Cybercrime: Networking Legal Systems in the Networked Crime Scene. Webology, vol. 4, no. 3, pp. 1−15.

Li, X. 2008a. Cybercrime and Deterrence: Networking Legal Systems in the Networked Information Society. Turku, Finland: University of Turku.

Li, X. 2008b. The criminal phenomenon on the internet: Hallmarks of criminals and victims revisited through typical cases prosecuted. *University of Ottawa Law & Technology Journal*, vol. 5, nos. 1-2, pp. 125-140.

Li, X. 2009a. Cyberstalking: Information and Communications Technology Makes it Different. ICFAI Journal of Cyber Law, vol. 2009, no. 1, pp. 5−10.

Li, X. 2009b. Spyware, Spy Affairs and Anti-Spy Actions. ICFAI Journal of Cyber Law, vol. 2009, no. 5, pp. 15−20.

Li, X. 2010. Cyber Warfare: Jokes, Hoaxes, or Hypes. The IUP Journal of Cyber Law, vol. 2010, no. 9, pp. 7−16.

Li, X. 2014. Phenomenal exploration into impact of anonymity on law and order in cyberspace. Criminology & Social Integration Journal, vol. 22, no. 2, pp. 102−123.

Li, X. 2016. Cybersecurity and Cybercrime in the 21st Century. Helsinki, Finland: Informyth.

Lilley, P. 2002. *Hacked, Attacked, and Abused: Digital Crime Exposed*, London, U. K.: Kogan Page Limited.

MacKinnon, R. C. 1997. Punishing the Persona: Correctional Strategies for the Virtual Offender, in S. G. Jones. (ed.). *Virtual Culture: Identity and Communication in Cybersociety*, London: SAGE Publications, 1997, pp. 206-235.

Maiwald, E. 2003. *Network Security: A Beginner's Guide*, second edition, California: McGraw-Hill Osborne Media.

McConnell International. 2000. Cyber Crime . . . and Punishment? Archaic Laws. Retrieved 5 May 2016, from http://www.witsa.org/papers/McConnell-cybercrime.pdf.

McNamara, J. 2003. *Secrets of Computer Espionage: Tactics and Countermeasures*, John Wiley and Sons.

Molnar, J. 1987. Putting Computer-related Crime in Perspective, *Journal of Policy Analysis and Management,* volume 6, number 4, Privatization: Theory and Practice, pp. 714-716.

Negroponte, N. 1995. A Bill of Writes, *Wired 3.05*.

Nycum, S. H. 1983. Testimony on Computer Security before the U. S. Senate Subcommittee on Oversight of Government Management of the Committee on Governmental Affairs, *Computers and Society*, volume 13, number 4 and volume 14, Nos. 1, 2, and 3.

Parker, D. B. 1976. *Crime by Computer*, New York: Charles Scribner's Sons.

Parker, D. B. 1980. Computer Abuse Research Update, *Computer/Law Journal*, vol. II, no. 2, pp. 329-352.

Philip, A. R. *The Legal System and Ethics in Information Security*, SANS Institute, 2002. Retrieved 5 May 2016, from http://www.securitydocs.com/go/1604

Pihlajamäki, A. 2004. *Tietojenkäsittelyrauhan rikosoikeudellinen suoja: datarikoksia koskeva sääntely Suomen rikoslaissa* (The Protection of Data Processing under Criminal Law: Provisions on Data Crimes in the Finnish Criminal Code), Helsinki: Suomalainen lakimiesyhdistys.

Pipkin, D. L. 2002. *Halting the Hacker: A Practical Guide to Computer Security (with CD-ROM)*, Englewood Cliffs, New Jersey: Prentice Hall PTR.

Police Commissioners' Conference Electronic Crime Working Party. 2000. The Virtual Horizon: Meeting the Law Enforcement Challenges: Developing an Australasian Law Enforcement Strategy for Dealing With Electronic Crime. Scoping Paper, Adelaide: Australasian Centre for Policing Research, Report Series No: 134.1.

Reece, D. 3 December 2000. The Hacker Cracker, The Sunday Telegraph, volume 14.

Rees, A. 2000. ACPR Technology Environment Scan, Report number 133.1, Adelaide: Australasian Centre for Policing Research.

Sieber, U. 1996. Computer Crime and Criminal Information Law - New Trends in the International Risk and Information Society - Statement for the Hearing on Security in Cyberspace of the United States Senate, Permanent Subcommittee on Investigations, Committee on Governmental Affairs, 16 July.

Sieber, U. 1998. Legal Aspects of Computer-Related Crime in the Information Society, The COMCRIME-Study for the European Commission. Retrieved 5 May 2016, from http://ec.europa.eu/archives/ISPO/legal/en/comcrime/sieber.html

Sjögren, H.; Skogh, G. 2004. Introduction, In Hans Sjögren and Göran Skogh eds. New Perspectives on Economic Crime, Edward Elgar Publishing, pp. 1-4.

Smith, R. G.; Grabosky, P.; Urbas, G. 2004. *Cyber Criminals on Trial*, Cambridge: The Press Syndicate of the University of Cambridge.

Solarz, A. 1981. *Computer Technology and Computer Crime*, Stockholm, Sweden: Research and Development Division.

Stephenson, P. 2000. *Investigating Computer-Related Crime*, Boca Raton: Florida: CRC Press.

Sterling, B. 1994. *The Hacker Crackdown: Law and Disorder on the Electronic Frontier*, Austin, Texas: Electronic Release. Retrieved 5 May 2016, from http://www.gutenberg.org/dirs/etext94/hack12.txt

Summers, D. (director). 2003. *Longman Dictionary of Contemporary English*, Essex, England: Pearson Education Limited.

Sutherland, E. H. 1949. *White Collar Crime,* New York: Holt, Rinehart and Winston.

Tavani, H. T. 2000. Defining the Boundaries of Computer Crime: Piracy, Break-ins, and Sabotage in Cyberspace, *Computers and Society*, volume 30, number 4, pp. 3-9.

Taylor, M.; Quayle, E. 2003. *Child Pornography: An Internet Crime*, East Sussex: Brunner-Routledge.

Technical Working Group for Electronic Crime Scene Investigation. 2001. *Electronic Crime Scene Investigation: A Guide for First Responders*, National Institute of Justice, Office of Justice Program, the United States Department of Justice.

Tennyenhuis, A.; Jamieson, R. 2003. Multidisciplinary E-Forensics Methodology Development to Assist in the Investigation of E-Crime, in Kim Viborg Anderson, Steve Elliot, and Paula M. C. Swatman, eds. *Seeking Success in E-Business: A Multidisciplinary Approach*, Norwell, Massachusetts: Kluwer Academic Publishers, 2003, pp. 187-206.

UNCJIN. 1999. International Review of Criminal Policy -United Nations Manual on the Prevention and Control of Computer-Related Crime, *International Review of Criminal Policy*, nos. 43 and 44.

Wasik, M. 1991. *Crime and the Computer*, Oxford: Clarendon Press.

Wells, T. D.; Sevilla, C. 2003. *Maximizing the Enterprise Information Assets*, Florida: Auerbach.

Yeager, P.; Clinard, M. 2006. *Corporate Crime*, Transaction Publishers.

Available online at jls.pruna.eu
Journal of Legal Studies
Journal of Legal Studies, 2016, 37–62
Received: 19 May 2016. Accepted: 19 June 2016. Published: 2 August 2016

公司法注册资本制度改革背景下

股东有限责任制度之反思与正当性重构[1]

张凌云♣

摘要：从历史渊源上追溯，所有权与经营权的分离是股东有限责任的经济基础，现代公司治理结构的成型是股东有限责任的制度基础。中国公司制度作为舶来品，缺少两权分离的经济现实和分权制衡的治理结构，这是思考中国公司法问题的事实前提。如果不能正确认识有限责任的法理基础和现实风险，不能充分估计中国商业环境的特殊性和复杂性，简单的“放松管制”和“朝底竞争”式的改革恐怕值得商榷。本轮注册资本制度改革弱化了股东出资义务，在有限责任和无限权力结合的基础上加剧了公司治理“权力-责任-义务”的结构性失衡，从根本上动摇了有限责任制度的正当性基础。笔者提出，为了重塑有限责任制度的正当性基础，考虑由控制股东对公司债权人承担信义义务性质的信息披露义务作为享有有限责任的对价，以克服“有限责任风险”并重新实现公司法上的“权力-责任-义务”配置平衡。享有法定知情权的债权人可以更有效地参与债

[1]本文为中国国家社会科学基金青年项目“企业信用信息公示法律问题研究”（项目批准号 15CFX061）的前期成果。

♣中国政法大学民商法学博士，美国佛罗里达大学访问学者，国家法官学院民商事审判教研室讲师。

务人公司治理，重塑分权制衡的现代法人治理结构，为中国公司治理难题的解决提供新的契机。

关键词：注册资本制度改革；股东有限责任；两权分离；信息披露义务

Abstract: Tracing back historically, the separation of ownership right and management right composed the economic foundation of the shareholders' limited liability system, while the modern structure of corporate governance served as its institutional basis. We should agree on the factual premise that the Chinese corporate system as an imported institution lacks the right-separating arrangement and the power-checking structure before considering the Chinese corporate dilemma. The reform-fashion of deregulating and bottom-down racing has been questionable given that the jurisprudence basis and factual risk of limited liability are not taken into full account with the particularity and sophistication of Chinese commercial environment. The corporate registered capital reform has weakened the shareholders' obligation of capital contribution and further exacerbated the structural imbalance of "Power-obligation-duty" of the corporate governance. Thus the combination of limited liability with unlimited power has shaken the legitimacy foundation of the limited liability system. It is suggested in this article that controlling shareholders should be burdened with a fiduciary-nature disclosure duty to creditors as a consideration for their privilege of limited liability, so as to neutralize the "limited liability risk" and rebalance the corporate allocation of "power-liability-duty". Creditors entitled with the statutory information rights would be able to participate into debtors' corporate governance more effectively, which would reshape the modern structure of corporate governance and provide a new opportunity for solving the Chinese corporate governance dilemma.

Key Words: The corporate registered capital reform; Shareholders' limited liability; Separation of rights; Information disclosure duty

导论

2013年末的公司法资本制度改革对传统的公司法原理和制度形成了强烈的冲击，法定资本制下的几项基本法律规则都被动摇：公司设立不再有最低资本额的要求；注册资本取消了实缴的比例限制只需认缴；股东出资不需要有最低的现金比例；强制验资的要求被取消。这场改革由行政力量发起并主导，乘着十八届三中全会的东风以近乎颠覆的方式完成了公司资本制度的改革。这场猝不及防的立法变革激发了学术界和司法界如火如荼的讨论，焦点集中在如何应对裁判基准失范以及股东恶意利用资本制度的问题。

然而在过去两年的讨论中，公司法的基础问题似乎被相对忽略了：公司的本质特征是什么？法人要取得独立人格，股东要承担有限责任，要不要对价？如果没有对价，股东有限责任的正当性何在？如果连出资义务都没有了，股东对公司还有什么义务？这些问题能否回答好，不仅关系到资本制度改革的成败，而且关系到公司制度的存亡。有限责任制度是一把双刃剑，用得好能够迅速积累财富，提高社会经济资源的配置质量和效率；用得不好则可能适得其反，对公司法律的制度根基造成破坏。从历史渊源上检讨，有限责任并非股东理所当然的福利，对股东有限责任之正当性基础的反思有助于在改革背景下调整与重塑公司法制度的发展方向。

一、股东有限责任的历史渊源和理论基础

有限责任产生的历史前提是企业所有权与经营权的分离，这从商业组织的历史演变中可见端倪。[2]公司治理的基本结构围绕着两权分离来演变，经过数百年的变迁最终形成分权制衡的治理结构，保证两权分离下的法人形成独立的意思表示。两权分离的经济现实和分权制衡的治理结构决定了股东的有限责任，进而决定了公司的独立人格和独立财产。

---

[2] 参见王建文：《公司形态的发展路径——历史线索与发展规律的探求》，载《南京大学法律评论》，2005 年秋季号，第 79 页。

（一）股东有限责任的经济基础——两权分离的产生

有限责任的产生与所有权和经营权的分离密切相关。一般认为，1932 年伯利和米恩斯在《现代公司与私有产权》一书中首次提出了“两权分离”的概念，进而确立了两权分离的现代公司理论，[3]之后学界也一直将两权分离作为一种理论来研究。[4]其实这种提法忽略了两权分离的事实存在性质和历史演变进路。两权分离作为一种经济关系形式，是随着生产力的逐步发展而形成的，或者说是生产关系适应生产力的表现。法人制度在古罗马时期就产生了，但是有限责任的完全实现只是数百年的事，从无限责任向有限责任的转化经过了上千年，这个时间差就是所有权与经营权伴随生产力的发展而逐步分离的过程。按照马克思主义政治经济学的原理，生产力决定生产关系，生产关系又决定法律制度，这个原理可以比较准确地解释有限责任的普遍实现。

早在远古的血缘家族里，由于生产力极其落后，人们的劳动存在必然竞合，人身关系上相互制约，这决定了财产的共同共有制。当时尚未有财产权和法律责任观念，财产债务与人身债务之间没有区分，父债子偿、卖身抵债等盛行，这是绝对意义上的“无限责任”。[5]

到了罗马时代，出现了简单商品经济的萌芽，相应地罗马法上发展出一套完善的私法制度，尤其是各种组织和团体人格的兴起，成为后世法人制度的开端。[6]一般认为，合伙起源于古罗马，以家庭作坊的形式将物品和劳作集中到一起，表现为典型的所有权与经营权合一，全体合伙人

---

[3] 黄一义：《从两权分离到两权合流——美国公司治理 100 年》，载《新财经》，2005 年 2 月，第 84 页。

[4] 参见何自力：《“两权分离”理论新探》，载《理论与现代化》，1999 年第 3 期，第 20 页；仇书勇：《反思对现代公司“两权分离”理论的两种误解——以法学为视角的研究》，载《法学论坛》，2007 年 3 月第 2 期，第 120 页。

[5] 参见赵旭东：《企业法律形态论》，中国方正出版社 1996 年版，第 135 页。

[6] 在古罗马时期，具有团体人格性质的社会组织形式在当时只是一种事实存在，罗马法中始终未形成明确的法人概念及近现代意义上的法人制度。参见王勇：《团体人格观：公司法人制度的本体论基础——罗马法中的人格学说与中国现代企业制度建构》，载《北京大学学报》（国内访问学者、进修教师论文专刊），2001 年，第 247 页。

对外承担无限连带责任。[7]后世诸多以罗马法为蓝本的法律制度体系中，法人成员对法人承担直接责任乃是普遍现象，这是由奴隶社会整体落后的生产力水平决定的。

及至中世纪，随着商品经济的发展，产生了资本进一步聚合的需要。当时地中海沿岸的海上贸易十分繁荣，海上贸易的发展要求扩大投资规模，同时降低投资风险，因此易于集资又能分散投资风险的组织便在意大利和地中海沿岸城市中因运而生，典型的是合伙组织康曼达（Commenda）。康曼达是指某些贷款人将资本委托给资金不足的商人去经营海上贸易，当发生损失时，委托人仅承担以出资为限的有限责任，而受托人则必须承担无限责任。[8]在康曼达组织的基础上发展出了两合公司：无意于公司经营仅想获取投资利润的股东，以丧失公司经营管理权为对价取得了有限责任特权；希望控制公司但缺乏充足资金的股东，在取得了公司经营管理权的同时，也承担了无限责任的代价。[9]在这个阶段，所有权与经营权部分分离，进而产生了不完全的有限责任。

从中世纪的后期开始，以特许状方式设立的特许公司，得以在商事领域发展起来。早期的特许公司不过是中世纪特许行会组织的海外延伸，成员所享有的责任仍然与中世纪法人无甚区别。[10]随着海外贸易在地域和规模上的拓展，对资本聚集的要求进一步加强，后期的特许公司如荷兰东印度公司和英国东印度公司成为现代股份有限公司的先驱。在英国，股份有限公司的决定性因素——所有成员的有限责任，到 1662 年得以

[7] 参见王建文：《公司形态的发展路径——历史线索与发展规律的探求》，载《南京大学法律评论》，2005 年秋季号，第 70 页。

[8] 同上，第 70-72 页。

[9] 同上，第 73-74 页。

[10] 特许合股公司所享有的一种自中世纪法人制度以来一直存在的征税或费用摊派的权力，使得身为法人之公司不具备独立而完全的自我责任能力。参见虞政平：《法人独立责任质疑》，载《中国法学》2001 年第 1 期，第 128 页。

确立。[11]在 17 世纪后半期，彻底的所有权与经营权分离以及完全的有限责任在小范围内得以实现。

进入工业革命时代，社会化大生产与技术产业的急速发展亟需更大规模的资本聚集，没有巨额资本的推动，一系列的生产力变革都无法进行。同时，工业革命对资本及组织方式均提出了严重的挑战：资本不仅需要更大规模的募集，更需要有效的组织与使用，特许公司凸显低能无效。在此背景下，非经特许的公司或企业得以广泛地自发形成以满足大量资本集聚的需要，所有权与经营权的分离愈发成为生产关系的常态。为满足社会对有限责任的强烈要求，1807 年颁布的《法国商法典》首先规定了股份有限公司的形态，随后股份公司在全世界传播蔓延，成为现代商业组织的主要形态。[12]

综上可见，有限责任的发展不是空穴来风，其背后的根本动力是生产力（工业革命进程）决定生产关系（两权分离程度），生产关系决定法律制度（有限责任确立）。[13]有限责任的产生有着深刻的历史经济背景，尽管投资者对有限责任的需求一直存在，但直至相应的生产力发展出了相应的生产关系以后才有可能实现此种法律关系。

---

[11] 1662 年查理二世颁布了《关于破产者的宣告条例》，该条例规定，东印度公司、非洲公司和同样的 Joint Stock Company 的成员对于公司仅承担有限责任。参见王建文：《公司形态的发展路径——历史线索与发展规律的探求》，载《南京大学法律评论》，2005 年秋季号，第 77 页。

[12] 第一次工业革命的时间是 18 世纪 60 年代到 19 世纪中期，第二次工业革命的时间是 19 世纪中下期到 20 世纪初。从时间线索上可以推论，第一次工业革命推动了 19 世纪初法国商法典确立股份有限公司的形态，股份有限公司的迅速普及随后推动了 19 世纪中下旬开始的第二次工业革命。参见虞政平：《法人独立责任质疑》，载《中国法学》2001 年第 1 期，第 128-129 页。

[13] 人类社会早期的人身性债务是真正的“无限责任”；相对而言，限定在个人财产上的无限责任即是进步的“有限责任”；而现代的有限责任制度将出资人责任限定在出资额之内，在实缴资本制下即相当于对公司随后的债务“无责任”。可见财产责任的发展呈不断限缩的历史趋势。

（二）股东有限责任的制度基础——现代法人治理结构的成型

上文通过历史考察说明了，生产力的发展决定了两权分离的经济关系，两权分离的经济关系又决定了有限责任的法律关系，这是“两权分离”和“有限责任”之间的历史逻辑。[14]在两权分离的背景下，股东有限责任在公司法上的真正确立与现代法人治理结构密不可分。如果说两权分离是股东有限责任的经济基础，那么现代法人治理结构就是股东有限责任的制度基础。与两权分离的历史演变相呼应的，是现代法人治理结构的历史演变进程。

早期的公司法理念认为，法律赋予了公司从事商事经营的资格或权力，公司作为一种私法上的自治组织可以自由行使公司权力，安排权利义务和利润分配等事宜，对于公司成员自己的事情法律不作强行规定。公司的成员就是股东，股东是公司的最终所有者，因而股东会也就是公司的最高权力机关，而董事会不过是股东的代理人并受到股东会的控制，这就是股东会中心主义。[15]早期西方各国基本上实行股东会中心主义，因为当时公司的规模尚小，股东持股的比例较大，两权分离的程度不高。从 19 世纪到 20 世纪初，各发达国家公司法均盛行股东会中心主义，股东会作为公司最高权力机关被确定下来，不承认董事会拥有独立于股东会的权力。[16]

进入 20 世纪，随着科技的进步和生产力水平的提高，大规模现代股份公司不断涌现。加之证券市场的日益发达，股份公司的股份高度分散并加快流转，两权分离的程度日益提高，这对股东会中心主义的治理结构提出了挑战。对于大量的中小股东来说，一方面他们力量微弱难以对公

---

[14] “两权分离”是历史进程中不可避免的经济现象，与其伴生的是“代理成本问题”，代理成本问题及其矫正在公司法学上已经得到了充分的研究。但是“两权分离”作为“有限责任”的经济基础，这两者的历史关系和逻辑联系相对被忽略了。

[15] 朱伯玉：《公司法人治理结构的历史演变及典型模式》，载《山东大学学报（哲学社会科学版）》，2001 年第 6 期，第 68 页。

[16] 韩长印，吴泽勇：《公司业务执行权之主体归属》，载《法学研究》1994 年第 4 期，第 83 页。

司的经营者施加影响，另一方面他们也缺乏足够的时间、精力和财力对公司董事实施有效监督。如此一来，“没有控制权的财产所有权与没有财产权的控制权是股份公司发展的逻辑归结。”[17]大多数国家的公司立法顺应这种变化，先后废除股东会中心主义而改采董事会中心主义。董事会代表股东行使公司权力，在公司运营中居于核心地位，一经公司章程把待定的权力授予董事会,股东会就不得干预他们行使此项权力。[18]

直至 20 世纪末，随着赋予公司董事会的经营者权限越来越多，董事会中心主义的弊端日渐显露，经营者所受到的监督远远低于其权限的增加，经营者的经营行为处于近乎监管失控的状态。值此契机，以美国为代表的西方主要发达国家自 20 世纪 80 年代末以来掀起了广泛的关于公司法人治理结构的大讨论，其间“利益相关者理论”逐渐占得上风。[19]按照利益相关者理论，公司的经营者除了对股东负责外，还应对非股东的利害关系人承担责任并接受其监督。在此背景下，当代公司法人治理结构的发展呈现出新的特点：例如设置公司监事会为代表的监督机构，要求董事会中有多数外部董事，职工参与制度受到重视，银行等金融机构在法人治理中的地位日渐增强等。

至此，建立在“分权”基础上的现代法人治理结构基本成型：股东会（股东大会）是权力机关，董事会是决策机关，监事会（独立董事）是监督机关，三权分立的治理结构保证法人独立意思的形成。同时，中小股东、债权人、职工等利益相关者的充分参与能够保证公司自治的过程不被控制股东和管理者的私利所异化。两权分离是现代公司治理结构成型的经

[17] Adolf A. Berle & Gandiner C. Means, The Modern Corporation and Private Property[M], Harcourt Brace Jovanovich, New York, 120(1963).

[18] 马俊驹、聂德宗：《公司法人治理结构的当代发展——兼论我国公司法人治理结构的重构》，载《法学研究》2000 年第 2 期。

[19] 朱伯玉：《公司法人治理结构的历史演变及典型模式》，载《山东大学学报（哲学社会科学版）》，2001 年第 6 期，第 69 页。

济基础，现代法人治理结构的设计充分体现了分权制衡的理念，[20]这构成了股东有限责任的制度基础。

一方面，股东有限责任的形成迫使法人责任因与股东责任分离而必然走向责任独立；另一方面，股东有限责任的前提是股东真实完整地履行出资义务，股东出资最终形成了公司的独立财产。因此，股东有限责任的完全实现促成了公司独立责任和独立财产的形成（股东有限责任决定了法人的独立责任，而不是法人人格决定法人独立责任），最终促成现代公司法人制度的成型。

总结之，公司的独立责任因股东的有限责任而成立，股东有限责任的正当性基础则在于两权分离的经济现实和分权制衡的治理结构。在这样的理论视野下，我们能够更清楚地观察中国公司“有限责任”的现实处境。

二、股东有限责任的现实悖论

（一）中国公司的发展缺乏两权分离的经济现实

纵观近代中国公司制度的演进，如果撇开最早出现的外国公司，其起点是官督商办的工矿业公司的产生（19 世纪 70 年代起），经由从家族企业到股份制企业的兴起，其终点也正好是国有垄断性大公司的阶段（1945 年抗战胜利之后）。这种从“官办公司”开始，又到“官办公司”告一段落的历史进程，是近代中国公司制度的一大特色。[21]历史的发展无

[20] 根据两权分离理论，所有权与经营权的分离，便产生了一种对资产的委托——代理关系：即资产的所有者不再直接经营企业，而是委托他人去经营管理。作为受托者，则是代理所有者从事生产经营。股份有限公司被划分为三个部分，即公司重大事项的决定权、公司经营业务的执行权以及公司经营活动的监督权。上述三项权力分别由不同的机关——股东会、董事会和监事会负责行使。股东会、董事会与监事会的结构，成为公司法人治理结构的典型形式。参见赵琴：《公司治理结构的历史演变及对我国公司治理结构的对策思考》，载《内江师范学院学报》2004 年第 19 卷第 5 期。

[21] 近代中国最早出现的公司是通商口岸一些由外国人开办和经营的公司。从 19 世纪 70 年代起，以官督商办、并且采取股份公司组织形式的轮船招商局的创办为标志，由中国人自己创办的工矿业公司开始逐渐增多。进入 20 世纪以后社会环境迅速变化，各类公

独有偶，这些垄断性的官办资本公司在建国后被重新国有化，成为新中国国有企业的基础，改革开放后这些国有企业通过国企改制成为了国有控股、相对控股、参股公司，并成为第一批上市公司的主力。与此同时，民营公司大多采取家族企业的形式发展，在经济体系中处于附属地位。

从这个简单的历史回溯可见，中国的公司制度作为舶来品，从近代到现代的演进历史都是由“国有”、“国营”力量主导的。然而从世界范围内的实际发展看，公司制度从一开始就是与私有制相联系、相适应的经济组织形式。在私有制下，由于其内在的利益驱动机制，公司制度会在具体运作过程中自然而然地发育演变，以自身的力量逐步成熟与纠错。而在复杂动荡的历史背景下，中国公司制度的生长始终是以“国有”力量和行政手段为主导，承载了市场发育和经济发展之外的使命，产生了诸多问题。[22]

与国有资本主导相关，国有公司的典型特点是“一股独大”，即便是上市公司也不具备两权分离的特征。[23]国家股一股独大的大股东是国家，股

司的设立进入了一个新的发展阶段，其中最具代表性和重要意义的是近代中国一些最为著名的家族公司。家族公司最主要的特征是公司资本的主要来源以及公司管理经营的家族化，无论是公司的创办、投资还是创办以后的具体经营管理，家族都在公司中占有主导的力量。20 世纪 40 年代抗日战争期间，各地方政府以股份有限公司的形式创办了各种省办企业，同一个公司名义下往往直接、间接地参与和掌握数量不等的跨行业、跨地域的下属公司。近代中国公司制度演进的最终阶段是 1945 年抗战胜利之后的国有垄断性大公司的发展阶段。20 世纪 40 年代之后，在抗战期间经营的国有企业以及战后接收敌伪产业基础上最终形成的国有垄断性大公司，不仅在数量上而且在公司的发展形态上，都远远超过了以往任何一个历史时期。参见张忠民：《近代中国公司制度的逻辑演进及其历史启示》，载《改革》1996 年第 5 期。

[22] 国有公司为主导的模式在理论和实践上都有一系列需要探索和解决的问题，例如：国家如何寻找和安排国家的代理人，国家的所有权如何得到最终的保证和体现，国有财产的法人财产治理结构如何安排，国有公司的内部管理如何进行，如何解决国有公司内部高昂的代理成本问题等等。这些问题在实践中并没有得到很好的解决。

[23] 为了保持公有制的主导地位，当国有企业进行公司制改造时，采取了国有股占绝对多数的做法，保留了上级机关对企业的支配地位；在上市指标分配上则通过行政手段向国有企业倾斜，致使实际得到上市公司资格的大多数都是国有企业，股票市场不是追求资源的最佳配置，而是被赋予了支持国有企业改革的职能。

东代表是政府部门，存在所有者缺位问题。大股东成为上市公司的主管部门，股东会、监事会形同虚设。大股东代表的公司控制权主体与剩余风险的承担主体不一致，不利于对大股东代表的约束和激励，其后果表现为大股东侵占上市公司资产，以上市公司名义为自己担保，关联交易泛滥，会计信息失真，非法挪用募集资金，损害中小股东的权益，上市公司的亏损比例逐年上升等。不单是国有公司，以家族企业为代表的民营公司也存在“一股独大”的问题。[24]家族公司最主要的特征是公司资本的主要来源以及公司管理经营的家族化，控制股东同时操纵股东（大）会、董事会和监事会，公司治理结构往往形同虚设。“自然人一股独大”具有极强的动机侵害中小股东的利益，其在公司决策中一言九鼎，出了问题却以股东“有限责任”一推了事，严重损害债权人利益。可以说，无论是国有公司还是民营公司，均未能成功实现现代公司治理转型。

公司制度演进的历史经验告诉我们，现代企业制度建设是一个按其自身发展规律逐步展开的自然历史过程，而不是毕其功于一役的运动。综观动荡曲折的中国近现代历史，公司制度难得有自由生长发育的土壤，比较稳定的历史时期也就是改革开放以后的这三十多年。其间受到历史变化的制约，公司制度的生长发育并非靠自然演进，而是靠顶层设计和政策式立法构造出来的。不可否认的是，中国公司的历史发展缺乏两权分离的经济基础，这是我们思考中国公司治理问题的事实前提。

（二）中国公司尚未建立分权制衡的治理结构

在一股独大的中国式公司中，法人的治理结构均存在不同程度的问题。

---

[24] 世界各国近代公司制度的演进过程中，几乎都有一个家族公司的发展时代。但是随着时间推移，家族公司的家族特性必然会逐渐淡化，那些规模较大的家族公司早晚都会走上社会化程度更高，资本的所有权和经营权分离更为彻底的发展道路。中国的公司发展史是个例外，一方面从历史发展的大跨度而言，家族公司还缺乏足够的展开时间和空间，家族公司向社会化程度更高、资本所有权和经营权分离更为彻底的演进还未能得到更为充分的展开；另一方面中国人特殊的宗族观念、血缘文化也制约着家族企业向现代治理结构的转型。参见张忠民：《近代中国公司制度的逻辑演进及其历史启示》，载《改革》1996 年第 5 期。

很多小微公司没有按照公司法的规定设立相应的组织机构，即便是设立了股东（大）会、董事会和监事会等法定公司机关，在商事实践中能形成有效的分权制衡机制的也为数甚少。中国公司法人治理结构极不完善，主要表现为缺乏有效的制衡监督制度。

在内部监督方面，监事会和独立董事往往形同虚设。[25]大陆法系的监事会制度和英美法系的独立董事制度被中国公司法双双吸收，但是均未发挥出应有的效果。“一股独大”的股权结构使得控制股东手握大权，可以随意操纵董事会、监事会及独立董事的任免，实际上将内部监督机制架空，使其无法发挥公司自治防弊的功能。在一股独大的公司里，由大股东委派的监事会不可能起到监督股东会的作用，由大股东委任的独立董事也不可能真正独立于“内部人控制”。在外部监督方面，中国公司缺乏债权人参与治理的制度。英美法系的“相机治理制度”和大陆法系的“主银行制”为债权人提供了对控制股东施加外部约束的机会，[26]但是中国公司法并没有提供债权人参与公司治理的制度激励。

公司治理的基本结构是围绕两权分离而产生的。分权制衡的治理结构，保证两权分离下的公司形成独立的意思表示，构成股东有限责任的现实基础；不完善的治理结构，则会导致公司与股东的组织机构、财产、人

---

[25] 独立董事制度和监事会制度分别来自英美法系和大陆法系，被 05 年公司法双双吸收进而融合成我国独特的内部监督制度。独立董事是指不在公司担任除董事职务以外的其他任何职务并与其所受聘的上市公司及其主要股东不存在可能妨碍其进行独立客观判断的一切关系的特定董事。监事会是指依法产生的代表全体股东对董事和经理的经营管理行为及公司财务进行监督的常设机构。参见赵旭东：《公司法学》（第二版），高等教育出版社 2006 年版，第 391 页。

[26] 美国相机治理机制的基础是企业所有权的状态依存特征。当企业在运营过程中显露出经营危机的苗头时，债权人作为利益相关者可以按照法定的程序要求重新分配控制权，例如改选董事会、更换管理层等。大陆法系的债权人治理模式以日本的“主银行”制度和德国的“全能银行”制度为典型。主银行和全能银行对公司治理的参与均基于股权和债权的双重身份，通过稳定的银企关系对客户企业同时施加内外部制约。相较之，德国的“全能银行”相比日本的“主银行”拥有更强的控制权。参见丁广宇：《论有限责任公司债权人权利的回归——基于相机治理理论的探讨》，载《法商研究》2008 年第 2 期，第 88 页。

员混同，进而可能适用法人人格否认，股东不再受有限责任保护。中国公司生态没有两权分离的经济现实，单纯复制西方的公司治理结构只能是空中楼阁；没有分权制衡的现代法人治理结构，泛滥的“有限责任”将成为制度性风险的元凶。公司法文本与实践样态的割裂是公司内部监督机制失范的原因，被割断了历史渊源和法理逻辑的有限责任制度成为诸多乱象的根源。

（三）有限责任风险

中国公司实践没有所有权与经营权分离的经济现实，没有分权制约的现代公治理结构，却规定了有限责任，这种搭配埋藏着深刻的矛盾，决定了大部分公司中权力与责任配置的错位。一方面，“公司自治”表现为“股东自治”，大部分公司都是由所有者经营（owner-managed），控制股东同时操纵股东（大）会、董事会、监事会等公司机关，掌握着公司一切的权力。另一方面，按照公司法的规定，“一股独大”的股东仅承担有限责任。因此，按照中国公司法的制度设计，控制股东同时享有“无限权力”和“有限责任”。

理论上，这种无限权力与有限责任的结合是荒谬的。公司自治是公司最基本的权力规则，有限责任是公司最基本的责任规则。在中国公司实践中，权力与责任的基本配置均偏好于控制股东，这种失衡的“权力-责任”结构必然引发“有限责任风险”，即控制股东必然会滥用股东有限责任（公司独立人格）向债权人转嫁风险。可以说，这种“有限责任风险”是一种由制度缺陷所决定的制度风险，而不仅仅是个别股东的道德风险。[27]在欺诈盛行的中国商业环境中，缺陷的公司制度和失衡的“权力-责任”

[27] 笔者认为中国公司的有限责任风险是一种制度性风险，原因有二：第一，从历史发展的纵向角度看，该风险是由中国公司发展的制度缺陷（权力–责任结构失衡）所决定的；第二，从公司制度的横向对比看，中国公司的有限责任只有形式对价，缺乏有效的实质对价。三权分立的组织结构要发挥效果建立在公司内部分权的基础上，对于所有权与经营权合一的公司而言，这种分权机制只是一种形式，无法构成有限责任的实质对价。

配置成了助纣为虐的帮凶。中国缺少诚信的商业文化很大程度上是被瘸了腿的“有限责任制度”放大了。

试想，我国的公司制度是以国有垄断公司形式发展起来的，却盲目引进西方在私有制基础上发展出来的公司法传统；我国的公司大部分都不具备两权分离的典型特征，却盲目引进国外在分权基础上设立的制度。或许这就是中国公司治理出问题的根本症结所在。中国没有发育出两权分离的经济现实，未建立在分权基础上的内部监督制度必然是无法奏效的；现代中国的企业制度演进需要足够的时间和空间来展开，盲目引进域外公司制度无法立竿见影地解决问题。如果不能正确认识有限责任的法理基础和现实风险，不能充分估计中国商业环境的特殊性和复杂性，简单的“放松管制”（Deregulation）和“朝底竞争”（Bottom down）式的立法恐怕将误入歧途。

三、注册资本制度改革背景下股东有限责任的困境

（一）注册资本制度的改革弱化了股东的出资义务

某种程度上，2013 年末公司法资本制度修改对现行公司法制度的冲击不亚于 2005 年公司法修改时资本制度的突破，横亘在公司设立者面前的最低注册资本的门槛没有了，把守资本真实性的验资关口也被撤除了，注册资本成了不需要即时兑付的空头支票。多年来习惯于严格资本管制和出资约束的投资者，在失去规则枷锁的同时，也迷失了能够快速摸清交易对方信用状况和责任能力的途径。与此同时，一系列严峻、现实的问题拷问着中国的公司法实务：新资本制度下股东是否还负有出资义务与责任？股东出资是否还有真实性与适当性的法定要求？是否还存在虚假出资与抽逃出资的违法行为？[28]

---

[28] 赵旭东：《资本制度变革下的资本法律责任——公司法修改的理性解读》，《第三届公司法司法适用高端论坛论文集》2014 年 5 月，第 29 页。

理论上而言，此次注册资本制度改革并没有动摇法定资本制的根基，资本真实性的要求并没有变。取消最低注册资本，改变的是股东出资义务的范围，而非股东出资义务本身；采用认缴资本制，改变的是股东履行出资义务的时间，没有否定股东履行出资义务；取消验资的法定程序，改变的是资本真实的实现方式，而非否定资本真实性的法律要求。但是从司法实务的角度而言，被取消的这些规则恰恰是以前司法实务赖以作出裁判的主要基础，例如最低资本额、出资比例、出资时间等，这直接影响到了认缴制采用以后瑕疵股东出资责任的裁判基准问题，为司法适用带来极大的不确定性。例如取消验资程序后如何认定股东履行了出资义务？债权人如何行使对未实缴股东的请求权？在出资义务不确定的情况下划分股权的依据是什么？如何解决相应的证据规则适用和证明责任分配问题？这些法律适用的灰色地带为当事人机会主义的出资行为留下了空间。

在我国不诚信的商业环境下，指望股东能如约履行出资义务的可能有多大？相当一部分出资人会选择恶意逃避出资义务，实践样态中股东出资义务的履行变得不确定。[29]如果连出资义务都没有了，那么股东对公司还有什么义务？股东有限责任的根基又何在？股东出资义务的弱化将损害公司的独立财产，进而损害公司独立承担责任的基础，造成公司对外承担责任的障碍。

（二）股东出资义务的弱化加剧了“权力-责任-义务”的配置失衡

如前文所述，在中国公司缺乏两权分离的经济现实和分权制衡的治理结构的环境下，股东无限权力与有限责任的结合必然引发“有限责任风险”。在“权力-责任”失衡的基础上，出资义务的弱化进一步加剧了“权力-责任-义务”的配置失衡，有限责任对应无限权力和不确定的义务。公司资本

[29] 从工商行政管理部门发布的数据看，注册资本制度改革以后设立“一元公司”和“亿元公司”的现象屡见不鲜。更有甚者随意更改注册资本，某注册资本 2000 万的投资公司（实缴出资 400 万）在新《公司法》股份认缴制出台后增资到 10 个亿，在签订近 8000 万元的合同后面对到期债务突然减资到 400 万元，引发相关纠纷。参见：《上海法院首例注册资本认缴出资案判决》，上海市普陀区法院网站。

是公司人格独立的必要条件，公司资本的形成使得公司财产独立于股东的财产，从而在法律关系上将股东财产与公司财产区隔开来；真实履行出资义务是股东承担有限责任的前提条件，如果股东只认缴而不实缴注册资本，理论上股东不应享有与注册资本相应的有限责任利益。在没有配套措施跟进的情况下，本次注册资本制度改革单纯弱化了股东的出资义务，降低了资本真实性要求，无疑将使本已倾斜的公司治理天平更趋不平衡。

股东有限责任的前提是股东真实完整地履行了出资义务，股东要真实履行出资义务是股东有限责任的题中之义。面对社会诚信状况的窘迫和债权人利益保护机制的脆弱，公司法在拆除最低资本标准和附期限实缴要求的法律屏障的同时，并没有提供配套的制度支持，给司法实践造成诸多困惑和难题。同时，资本制度改革所造成的股东出资义务不确定很可能进一步放任欺诈之风大行其道。[30] 出于控制交易风险的考虑，银行等债权人会更多地运用股东个人担保的方式，公司的有限责任基础进一步削弱，这恐怕和改革者的意图背道而驰[31]。在法治建设过程中借鉴和移植别国制度建设经验十分重要，但同时需要我们结合本国实际状况进行判断和选择。罔顾我国商业诚信环境很差的国情和公司制度的特殊性，改革者所期望的“投资能量释放”很可能种下“公司信用恶化”的恶果，并

[30] 全国人大常委会 2014 年 4 月 24 日对刑法 158 条、159 条作出了立法解释：刑法第 158 条、159 条只适用于依法实行注册资本实缴登记制的公司。在全国人大常委会修改了虚报注册资本罪、虚假出资、抽逃出资罪的适用范围之后，企业抽逃资本就少了刑法上的约束。实际效果是进一步弱化了资本真实性的要求，也动摇了股东有限责任的正当性基础。

[31] 司法实践当中有限责任无限化的趋势正在加强。银行放贷时不仅要审查各方面的财务资料，而且要求股东个人全部要担保，相关情况的变化要及时告知银行，交易中的尽职调查、资产评估、对股东、高管责任的要求等均有所加强。与此同时，有些优质借款人属于高度风险保守型，不愿意将个人财产置于公司破产的风险之下，此时股东拒绝提供个人担保可能因此丧失获得贷款的资格；而有些劣质借款人属于高度风险偏好型，尽管其没有为公司债务承担个人责任的意愿，依然会同意个人担保条款以获得贷款，事后再通过财产转移、欺诈转移等手段逃避债务、转嫁风险。

且可能对公司法的基本制度造成破坏性的影响。[32]

四、股东有限责任的正当性重构——控制股东对公司债权人的信息披露义务

中国公司环境缺乏两权分离的经济基础和分权制衡的治理结构，盲目引进西方在分权基础上建立的公司制度产生了诸多问题。一方面，有限责任与无限权力的配置失衡导致了制度性的“有限责任风险”的泛滥。另一方面，在注册资本制度改革的背景下，股东出资义务的弱化和资本真实性要求的降低进一步为中国投机性的商业环境增加了不确定的因素。因此有必要思考：如何遏制有限责任的制度性风险？如何在改革背景下调整和重塑公司法制度逻辑？如何重构股东有限责任的正当性基础？

（一）控制股东对公司债权人的信息披露义务——重新平衡“权力-责任-义务”配置

股东有限责任制度正当性重构的关键在于有效化解有限公司的“有限责任风险”，要化解“有限责任风险”首先要平衡有限公司中失衡的“权力-责任”配置。目前的主要手段是通过法人人格否认制度和股东个人担保等途径实现有限责任无限化，进而扩大股东的责任范围。然而，法人人格否认是以法官自由裁量权为基础的个案衡量制度，在司法适用层面存在重重问题，实际上无力纠正此种制度缺陷造成的系统风险。单纯通过股东个人担保突破有限责任规则会产生扭曲的经济效果。[33]加之在我国企

[32] 英美授权资本制下维护交易安全的配套制度非常完备和精细，我国则缺乏那种系统性的法律配置和软文化。美国公司制度在无最低资本要求体制下依靠商业透明度、社会信用体系、公司经营状态压力测试、董事责任、揭开公司面纱、诉讼审查关联交易、股东债权衡平居次等规则，有效防止了不诚信的股东利用公司控制权和有限责任对债权人利益造成不正当侵害。英美法系的这一套资本制度体系，与我国的国情、资本信用规则、商业传统、商人意识、司法认知、法治文化相去甚远。参见甘培忠：《论公司资本制度颠覆性改革的环境与逻辑缺陷及制度补救》，《第三届公司法司法适用高端论坛论文集》2014 年 5 月，第 44 页。

[33] 公司经营本就面临着风险，即便经营者谨慎履行善意勤勉的义务，公司仍不可免除因正常商业风险造成经营失败而宣告破产的可能。为公司债务提供个人担保就意味着股

业失信惩罚机制缺位，违法违约成本过低，恶意逃债的股东似乎成了有限责任制度的最终受益者。要有效应对此种因有限公司制度缺陷造成的系统性风险，就必须对症下药，以一种制度性的方式改变有限公司“权力-责任-义务”配置结构。通过向公司的控制股东施加法定义务，以平衡无限权力与有限责任的冲突，让控制股东为“有限责任”付出足够的“义务对价”。笔者认为，由公司控制股东对债权人承担信义义务是一种可行的理论设想。

按照 Weinrib 教授提出的信义义务之权力和自由裁量理论（the power-discretion theory），当一方具有自由裁量权，而信任其正当行使权力的另一方可能被权力滥用所损害的时候，前者就对后者负有信义义务。[34] 此种信义义务的结构与公司债权人和债务人的关系相吻合，公司控制者拥有通过公司自治改变债权人地位的自由裁量权，而信赖该自由裁量权正当行使的债权人可能遭受该信赖被滥用的侵害，这决定了公司控制者应当对债权人承担信义义务。公司法的基本权力规则和基本责任规则都默认设置为有利于公司的控制股东，通过设置第三个默认规则——公司控制股东对债权人的信义义务——作为公司的基本义务规则，可以有效抗衡控制股东的滥权行为，进而平衡“权力-义务-责任”配置关系。[35]

实际上，信义义务的概念具有极大的模糊性和适用弹性，只要具备了基本的信义结构（保护受益人的信赖免受自由裁量权之滥用，以及义务之违反产生相应责任），董事对债权人信义义务的具体内容可以根据债权人的具体需要来解释。不同于中小股东缺乏参与公司治理博弈的能力或

东完全放弃了有限责任保护，不区分恶意违约或正常风险。经常出现的情况是，善意借款人（提供了个人担保）要因正常经营风险而承担个人责任，而恶意借款人（未提供个人担保）则可以从事投机行为并从容摆脱公司债务。这样的有限责任只保护恶意借款人，效果如同要求善意借款人去“补贴”恶意借款人。这就产生了“逆向选择”问题，无法从根本上化解“有限责任风险”。

[34] R. Flannigan, ""The Fiduciary Obligation" (1989) 19 Oxford Journal of Legal Studies, 285, 308.

[35] 此种信义义务会使债权人与债务人公司之间的债权契约发生性质的变化，从力图对各种或有事件作出详尽安排的相机合同（Contingent contract）转变为类似股东与公司之间以信义关系处理不确定性的关系合同（Relational contract）。

动力，债权人通常具有极强的通过合同对借款人施加控制并依或有事件之触发参与公司治理的能力。换言之，债权人不需要象股东那样被信义义务全面保护。那么，债权人能力的“短板效应”（Cask Effect）在哪里呢？作为公司的外部人，债权人在获取公司内部信息的能力上具有明显的缺陷，尤其在实时追踪公司资产之动态演变方面（公司资产信用的变化）力不从心。公司资产是公司债务的一般担保，公司资产信息（动态或者静态）是债权人作出发放贷款或者债务再谈判等决策时的首要参考因素，因而公司资产信息的真实性、准确性和及时性对债权人关系重大。然而公司管理层在资产信息披露方面通常采取延迟披露或模糊披露的方式以蒙蔽债权人，债权人因此蒙受损失，董事却无须为虚假披露承担责任。换言之，债权人不需要忠实义务和勤勉义务那般事无巨细的关照标准，只要保证真实、充分的信息披露，在及时掌握公司资产变动状况的基础上债权人有充分的手段保护自己的利益。因此，可以考虑把信义义务中包含的信息披露义务独立出来，作为一项单独的法定义务加以规定，即公司控制股东对债权人承担法定的信息披露义务。在信义义务性质的信息披露义务（Fiduciary-nature disclosure duty）之下，任何资产信息的虚假披露、不完整披露或延迟披露导致债权人受到损失的，将由过错董事及股东承担相应的个人责任。

这种信息披露义务在多国公司法上均有不同程度的体现。日本公司法的特点是保护债权人的查阅权，股份公司和合同公司的债权人可以随时查阅公司置备的股东大会会议记录、会计参与资料、财务会计报表、资产负债表等，甚至可以有条件地查阅董事会会议记录等，董事、高管等对第三人虚假披露要承担损害赔偿责任。[36]英国公司法的特点是完备详尽的登记规则，公司需要向登记官提交公司备忘录和章程、董事成员变化、年度账目、资产负债表、董事报告、审计报告、公司治理声明等完整的公司记录，同时债权人可以查阅登记的公司记录及其原始文件。[37]欧盟公司法指令对闭锁公司的信息披露义务亦有要求，各成员国应当确保其

[36] 日本 2005 年《公司法》第 318 条、第 371 条、第 378 条、第 429 条、第 442 条、第 496 条等。

[37] 英国 2006 年公司法《UK Companies Act 2006》第 116 条、第 423 条、第 431 条、第 441 条、第 744 条、第 877 条、第 1078 条、第 1085 条等。

辖内公司对公司章程、公司设立文件、实缴出资、公司机关组成人员及变动、每一会计年度的资产负债表、损益表及年度财务报告等文件和事项进行强行性公开。[38]

（二）在我国公司法上确立对债权人的信息披露义务——《企业信息公示暂行条例》的启示

在我国公司法的背景下，信息披露义务的确立对于债权人保护具有特殊的意义。近年来，我国的商业信用呈现总体整体恶化的趋势，会计信息失真和信贷数据造假的现象层出不穷。[39]与此同时，债权人获得信息的手段严重不足。通过合同来构造债权人知情权的交易成本过高，对于金融债权人之外的债权人不可行。而公司法上仅规定了在“合并”、“分立”、“减资”、“清算”四种情形下公司应当通知债权人并且在报纸上发布公告，并没有规定债权人有权利获取公司的资产信息，更没有规定知情权遭到侵害的救济手段。在我国特殊的国情下，债权人迫切需要得到信息权利方面的保护。有必要在我国公司法上确立对债权人的信息披露义务，让股东为“有限责任”付出足够的“义务对价”，进而平衡“权力-责任-义务”比例，遏制股东有限责任风险。

在此方面，《企业信息公示暂行条例》先行一步。2014年8月23日国务院公布了《企业信息公示暂行条例》（以下简称《条例》）,规定自2014 年10月1日起正式施行企业信息公示制度。《条例》试图构建统一的企业信用信息公示体系,形成企业“一处违法、处处受限”的信用约束机制。按照《条例》的规定，承担信息披露义务的主体包括企业、工商行政管理部门和其他政府部门。其中关于企业报送年度报告和临时报告的

---

[38] 欧盟第一号公司法指令第 2 条、第 3 条，第四号公司法指令第 2 条、第 46 条、第 47 条、第 48 条。

[39] 商业实践中，采取伪造、掩饰的方法在会计凭证、会计账簿、会计报表以及其他统计资料和业务活动记录材料上做手脚非常普遍；不仅假账盛行,各种假发票、假税票、假进账单、假报关单、假审计报告、假财务分析更是防不胜防；大多数企业向银行申请贷款时所提交的验资报告、评估报告和各种财产报告都是有水分的，编造虚假利润、伪造贷款凭证的现象比比皆是。

规定，实际上确立了公司向债权人披露信息的义务。[40]然而从商事法律的角度而言，还有诸多问题悬而未决：债权人可否要求查阅公司的财务会计资料？债权人因虚假披露遭到损害时可否提起知情权诉讼？诉讼的依据是什么？诉讼的性质是违约之诉还是侵权之诉？举证责任和证明标准如何确定？承担信息披露义务的主体是谁？承担虚假披露赔偿责任的主体是谁？可否要求控制股东和董事承担连带责任？赔偿范围如何界定？损失数额如何计算？信息披露与商业秘密保护的关系如何处理？《条例》从行政法规的层面确立企业披露信息的义务反映了改革直觉和实践智慧，但其中涉及到的复杂问题并非一部行政法规所能解决的。

实际上，信息披露义务作为公司的基本义务之一，涉及到公司法人的基本人权问题，有必要在商事组织法即公司法的层面上规定公司对债权人的信息披露义务，同时明确信息披露义务的范围。从比较法上看，公司的信息披露义务主要体现在两个方面，主动披露信息的义务以及就债权人提出的查阅要求提供相关信息的披露。笔者认为可以从以下几个方面构建我国公司法上的信息披露义务：

1、公司法应当适时确认公司负有及时公示企业信用信息的义务，实现与《企业信息公示暂行条例》的衔接。一方面，公司要通过年度报告定期公示企业信息（每年 1 月 1 日至 6 月 30 日），包括向潜在债权人（公众）公示企业存续状态信息、投资信息、认缴资本额、实缴资本额、出资时间、出资方式、股权变更、网络经营等信息，向现实债权人公示企业从业人数、资产总额、负债总额、对外提供保证担保、所有者权益合计、营业总收入、主营业务收入、利润总额、净利润、纳税总额等信息。另一方面，公司要通过临时报告不定期公示企业信息（自信息形成之日

[40] 按照《条例》第九条的规定，企业应当向社会公示如下信息：企业开业、歇业、清算等存续状态信息；企业投资设立企业、购买股权信息；股东或者发起人认缴和实缴的出资额、出资时间、出资方式等信息；有限责任公司股东股权转让等股权变更信息；企业网站以及从事网络经营的网店的名称、网址等信息。此外，企业从业人数、资产总额、负债总额、对外提供保证担保、所有者权益合计、营业总收入、主营业务收入、利润总额、净利润、纳税总额信息由企业选择是否向社会公示。经企业同意，公民、法人或者其他组织可以查询企业选择不公示的信息。

起 20 个工作日内），包括认缴出资额、实缴出资额、出资时间方式、股权变更、行政许可取得及变更、知识产权出质登记、所受行政处罚信息等。应当在公司法上尽快确认《条例》所规定的企业信息公示义务，确立因企业信息公示而生的商事纠纷的解决依据。

2、借鉴日本公司法典，明文规定我国公司法上的债权人查阅权制度。日本企业融资制度以主银行制为特色，主银行通过债权和股权的双重控制参与公司治理，为此日本公司法典赋予了债权人强大的查阅权，股份公司和合同公司的债权人可以随时查阅公司置备的公司章程、股东名册、股东大会会议记录、会计参与资料、财务会计报表、资产负债表等，同时可以有条件地查阅董事会会议记录、监事会会议记录、委员会会议记录等。[41]我国银行债权人的强势地位与日本的主银行类似，可以考虑适度借鉴日本公司法，规定符合一定条件的债权人可以查阅公司置备的会议记录、财务资料和审计资料等。债权人查阅权可以迅速满足债权人的信息需求，并直接遏制债务人公司隐瞒信息的机会主义行为，因此其理应覆盖各类资产信息，包括资产结构信息、资产状态信息、资产流动信息。[42]当然，为保护债务人公司的商业秘密和正当利益，债权人查阅权需要受到一定限制。

---

41 参见崔延花译：《日本公司法典》，中国政法大学出版社 2006 年第 1 版。第三十一条（公司章程的置备和阅览）、第一百二十五条（股东名册的置备和阅览）、第三百一十八条（股东大会会议记录之查阅）、第三百七十一条（董事会会议记录之查阅）、第三百七十八条（会计参与的财务会计报表等置备和查阅）、第三百九十四条（监事会会议记录之查阅）、第四百一十三条（委员会会议记录之查阅）、第四百四十二条（财务会计报表等的置备及阅览）、第四百九十六条（资产负债表等的置备及阅览等）、第六百二十五条（合同公司债权人阅览财务会计报表的权利）、第八百零一条（有关吸收合并等的书面文件等的置备及阅览等）、第九百五十一条（调查机关财务会计报告等的置备及阅览），等等。

42 资产结构信息即公司资产的构成状况，包括公司拥有的不动产（土地使用权、房屋所有权）、准不动产（机动车）、动产（生产设备、生产原料）、权利（股权、知识产权、债权）等的价值数额和相对比例。资产状态信息即公司资产的盈亏状况，包括利润率、净资产额、担保额等财务状况，还应包括查封、冻结、扣押等司法状况（属于广义的状态信息）。资产流动信息即公司资产的变动状况，包括合并、分立、减资、清算、赠与、借贷、担保、转投资、关联交易、资产重组、战略调整、风险营业增加等资产决

3、在公司法上确立虚假披露的责任追究机制——债权人知情权诉讼。为了保证公司债务人真实履行信息披露义务，可以借鉴日本公司法第429 条关于董事高管等对第三人虚假披露损害赔偿责任的规定，[43]由公司法对债权人知情权诉讼加以详细规定，包括知情权诉讼的提起方式、提起条件、举证责任、证明标准、赔偿范围、责任主体、连带责任等等。只有落实到民事责任和司法适用上，对债权人的信息披露义务才能真正实现遏制“有限责任风险”的功能。

面对商业信用恶化的严峻形势，信息披露义务以及企业信用信息约束机制的确立为改善中国公司治理问题提供了契机。在中国公司“一股独大”的股权结构下，内部监督制度设计（监事会、独立董事、中小股东监督等）往往难以奏效，必须寻找有效的外部力量即债权人加入公司治理的博弈。在确立公司债务人信息披露义务和债权人知情权诉讼的基础上，鼓励债权人通过适当的方式及时介入公司治理，[44]形成有效的外部监督

策。资产结构信息主要体现在资产负债表上；资产状态信息主要体现在资产负债表、现金流量表、利润表等财务文件中；资产流动信息会体现在公司机关的决议和财务会计报告中。因此，根据债权人不同的查阅要求，债务人公司应分别提供公司机关决议记录（包括股东会决议、董事会决议等）、财务会计报告（包括资产负债表、现金流量表、利润表和所有者权益变动表等）、以及公司章程等的查阅。

43 《日本公司法典》第四百二十九条：第一款：高级管理人员等（董事、会计参与、监事、执行官或会计监察人）就执行其职务存在恶意或重大过失时，该高级管理人员等承担赔偿由此对第三人造成的损害的责任。第二款：以下各项所列者，实施了该各项规定的行为时，亦同前款。但该人证明了就实施该行为未怠于注意时，不在此限。一、董事及执行官的下列行为：I 就募集股份、新股预约权、公司债或附新股预约权公司债认股人之际须通知的重要事项的虚假通知，或就供为该募集进行有关该股份公司事业及其他事项的说明之用的资料的虚假记载或记录。II 就应记载或记录于财务会计报表及经营报告以及这些文件的附属明细表以及临时财务会计报表的重要事项的虚假记载或记录。III 虚假登记。IV 虚假公告（包括以电磁方式进行财务会计报表的公告）。二、会计参与就应记载或记录于财务会计报表及其附属明细表、临时财务会计报表以及会计参与报告的重要事项的虚假记载或记录；三、监事及监查委员就应记载或记录于审计报告的重要事项的虚假记载或记录；四、会计监查人就应记载或记录于会计审计报告的重要事项的虚假记载或记录。

44 日本的“主银行”制度、德国的“全能银行”制度和美国的相机治理机制是目前债权人治理的典范，值得借鉴。主银行和全能银行对公司治理的参与均基于股权和债权的双重身

分权机制，此为遏制有限责任风险之逻辑，亦是重塑有限责任制度正当性之途径。

结语

长期以来，公司法学界不重视有限责任制度的基本研究，对股东有限责任的制度缺陷缺乏足够的认识和重视。实际上，我国公司普遍缺乏两权分离的经济现实和分权制衡的治理结构，以纯粹功利的态度利用“有限责任”释放投资能量，以信用环境的恶化为代价放任公司法制的畸形发展，长远看来后患无穷。公司数量的激增将带来经济繁荣不假，但不能忽略“有限责任泛滥”中暗藏的风险；放松管制、降低门槛的改革意图值得称赞，但不能忽略中国脆弱的商业环境中本已失衡的公司制度。如何改变公司的“权力-责任-义务”结构以克服“有限责任风险”？如何改革公司治理机制以实现有限责任制度的正当性重构？信息披露义务和信用约束机制的确立为攻克中国公司治理之顽疾开辟一条新的路径，是逻辑推理之结果，也是实践智慧之选择。作为商事主体的基本组织法，公司法必须及时回应自己的时代使命，确立公司债务人的信息披露义务以重塑公司的“权力-责任-义务”体系，引入债权人治理机制调控“有限责任”的制度性风险，通过制度激励改变公司的治理结构和信用环境，为企业信用约束机制和社会信用体系的建立打下坚实的公司法制基础。

参考文献：

Berle, A. A. & Means, G. C. 1963. The Modern Corporation and Private Property, New York: Harcourt Brace Jovanovich.

份，向客户企业派遣董事，通过稳定的银企关系对客户企业同时施加内外部制约。相较之，德国的“全能银行”相比日本的“主银行”拥有更强的控制权。美国的相机治理机制不具备这么紧密的银企关系。银行平常不会深入介入企业事务，基本上不干预企业的日常经营决策，只是按照债权契约进行惯例性的监督，如事前对借款企业的贷款风险、现金流、资信状况进行严格审查，事中要求借款企业及时呈报财务状况以掌握贷款项目的风险变化等。在客户企业出现巨额亏损、利润下降、重大事件等导致无法偿还到期债务时，银行才会深度介入企业甚至要求取得企业控制权。

Flannigan, R. 1989. The Fiduciary Obligation, Oxford Journal of Legal Studies, 9, 285–294.

仇书勇，《反思对现代公司“两权分离”理论的两种误解——以法学为视角的研究》，《法学论坛》2007年3月第2期。

崔延花译，《日本公司法典》，中国政法大学出版社2006年第1版。

丁广宇，《论有限责任公司债权人权利的回归——基于相机治理理论的探讨》，《法商研究》2008年第2期。

甘培忠，《论公司资本制度颠覆性改革的环境与逻辑缺陷及制度补救》，《第三届公司法司法适用高端论坛论文集》2014年5月。

韩长印、吴泽勇，《公司业务执行权之主体归属》，《法学研究》1994年第4期。

何自力，《“两权分离”理论新探》，《理论与现代化》1999年第3期。

黄一义，《从两权分离到两权合流——美国公司治理100年》，《新财经》2005年2月。

刘燕，《公司法资本制度改革的逻辑和路径——基于商业实践视角的观察》，《法学研究》2014年第5期。

马俊驹、聂德宗，《公司法人治理结构的当代发展——兼论我国公司法人治理结构的重构》，《法学研究》2000年第2期。

王建文，《公司形态的发展路径——历史线索与发展规律的探求》，《南京大学法律评论》2005年秋季号。

王建文，《公司形态的发展路径——历史线索与发展规律的探求》，《南京大学法律评论》2005年秋季号。

王勇，《团体人格观：公司法人制度的本体论基础——罗马法中的人格学说与中国现代企业制度建构》，《北京大学学报》（国内访问学者、进修教师论文专刊2001年）。

虞政平，《法人独立责任质疑》，《中国法学》2001年第1期。

张忠民，《近代中国公司制度的逻辑演进及其历史启示》，《改革》1996年第5期。

赵琴，《公司治理结构的历史演变及对我国公司治理结构的对策思考》，《内江师范学院学报》2004年第19卷第5期。

赵旭东，《公司法学》(第二版），高等教育出版社2006年版。

赵旭东，《企业法律形态论》，中国方正出版社1996年版。

朱伯玉，《公司法人治理结构的历史演变及典型模式》，《山东大学学报（哲学社会科学版）》2001年第6期。

Available online at jls.pruna.eu
Journal of Legal Studies
Journal of Legal Studies, 2016, 63–73
Received: 13 June 2016. Accepted: 4 July 2016. Published: 2 August 2016

启动国外民事诉讼程序

追讨海外腐败财产的法律问题研究

—以提起美国诉讼为例

刘鎏♣

摘要：中国政府目前加大了海外追赃力度，但是中国目前的追赃手段均存在着不足，急需进行创新。《联合国反腐败公约》第 43 条提出了一个新的启示，即启动国外民事诉讼程序追逃海外腐败财产。中国目前流去美国的腐败资产最为庞大，因此特以美国为切入点，在充分了解美国民事诉讼制度，尤其是管辖权制度的基础上，适时提起民事诉讼，也许能够为中国海外追赃工作打开新的局面。

关键词：海外；腐败资产；民事诉讼；美国

Abstract: The Chinese goverment puts forward higher requirements for the work against corruption, but those relevant measures taken by Chinese goverment now can not work effectively. The article 43 of UN Convention against Corruption provides a new approach, filing a civil litigation to claim for the recovery against corrupt assets in a judgment by the local courts. United

♣安徽师范大学法学院，法学硕士。主要研究方向：诉讼法。基金项目：安徽师范大学研究生科研创新与实践项目(一般项目)，编号(2015cxsj103)。

States is the main destination of the corrupt asstes flowing from China, thus we should file a civil lawsiut timely based on the full understanding of the civil litigation proceedings of United States, especially jurisdiction. This new endeavor will open up a new prospect for the work against corruption.

Keywords: Overseas; Corrupt assets; Civil litigation; United States

一、中国追讨海外腐败资产的困难与问题

中国共产党的十八届四中全会通过了《关于全面推进依法治国若干重大问题的决定》，将推进依法治国作为本次会议的主题，会议要求加强涉外法律工作，运用法律手段维护中国主权、安全、发展利益。会议要求坚定不移地反对腐败，深化法律合作和国际司法协助，加强反腐败国际合作，加大海外追逃追赃力度等，对中国今后海外反腐败工作提出了更高的要求。一般而言，在中国，作为唯一的执政党，中国共产党的政策对于国家的政策和法律具有指引作用，在十八届四中全会以后，中国政府明显加大了海外追赃追逃力度。

经过几十年的实践和摸索，中国海外反腐败合作的形式和手段呈现出多样化的特点，包括引渡、请求遣返、劝返、外国刑事判决的承认和执行、国际刑事合作以及跨境警务合作等等，在实践中，中国相关部门灵活运用上述手段，打击腐败犯罪，取得了显著的成就，有效地震慑了腐败犯罪分子。但是随着中国追赃力度的加大，在实践中，上述手段均在不同程度上呈现出一些不可克服的特点，例如中国在请求腐败犯罪分子所在国引渡该犯罪分子时，除受制于双方是否存在引渡条约这一前提外，还受制于本国人不引渡、政治犯不引渡、死刑不引渡等一系列原则的约束，往往导致中国大量的引渡努力的失败。另外，中国《刑事诉讼法》第234条规定：“公检法对查封、扣押、冻结的嫌疑人、被告人的财物及其孳息，应当妥善保管，……。人民法院作出的判决，应当对查封、扣押、冻结的财物及其孳息作出处理。人民法院作出的判决生效以后，有关机关应当根据判决对查封、扣押、冻结的财物及其孳息进行处理。对查封、扣押、冻结的赃款赃物及其孳息，除依法返还被害人的以

外，一律上缴国库。”但是在实践中，涉外海外腐败财产时，往往需要进行国际刑事合作，程序繁琐不说，而且犯罪分子或者腐败财产所在国也不一定会承认中国法院做出刑事判决的域外效力，这导致第234条在实践中发挥的作用非常有限。因此，为了有效地打击腐败犯罪，必须对追讨海外反腐败资产的工作进行创新。

《联合国反腐败公约》第43条给我们提供了新的思路，该条规定：各国在适当而且符合本国法律制度的情况下，缔约国应当考虑与腐败有关的民事和行政案件调查和诉讼中提供协助。这实际上为腐败行为受害国提供了一条新的救济途径，即直接在腐败犯罪分子所在国启动民事诉讼，请求所在国法院查封、冻结腐败财产，并要求将所涉腐败财产返还给受害国。事实上，《联合国反腐败公约》第五章将追回财产的法律手段划分为两大类,即:“直接追回财产的措施”和“通过没收事宜的国际合作追回财产的机制”。在被非法转移财产的发现地提起民事诉讼,是直接追回财产的最重要措施之一。在实践中，已经有几个国家尝试使用发起民事诉讼的方式追讨海外腐败财产，并且取得了不错的效果。

由于中国腐败资产大量流入美国，且美国秉承一套与中国截然不同的司法制度，因此，本文特以美国为切入点，探讨向美国法院发起民事诉讼追讨腐败资产的问题，希望能够为中国海外追赃工作带来新的思路，也为全球反腐败工作做出贡献。

二、美国追赃存在的困难与解决

中国与美国目前不存在双边的引渡条约，美国也不可能承认中国的刑事判决。在现实中，对于逃入美国的腐败犯罪分子，中国通常请求美国以非法入境为由予以遣返，并借此追讨赃物，但是这种努力能否成功取决于美国的态度，而且程序也较为繁琐，另外，如果犯罪分子获得美国绿卡或者国籍，那么美国便会直接拒绝遣返，使得所有努力化为泡影。因此，中国办案人员也会直接接触腐败犯罪分子，希望通过劝返的方式，让其主动投案自首。这种方式快捷高效，但也问题重重。首先，这需要

犯罪分子自身配合，如果犯罪分子在海外拥有大量资产，并且生活较好，他们不可能接受劝返；其次，办案人员深入美国寻找和接触犯罪分子，这对其人身也带来了一定的危险；最后，办案人员以公职身份进入美国进行劝返工作，这很容易引起误会和反感，甚至引起政治纠纷。

如果我们依据《联合国反腐败公约》第43条直接提起民事诉讼，则具有以下好处：第一，中美两国均为《联合国反腐败公约》缔约国，针对中国相关单位提起的诉讼，美国法院应当受理；第二，以启动外国民事诉讼的方式追讨海外腐败财产，只要能够掌握犯罪分子藏身之地或者腐败财产所在地即可，具有很大的可操作性；第三，这不受腐败犯罪分子是否入籍或者是否获得绿卡的影响，只要证明犯罪分子侵害了中国国家或者单位的财产权，或者能够证明中国对腐败资产拥有合法所有权即可；第四，相对于刑事司法协助而言，程序简便，追讨腐败财产的效率更高；第五，中国在请求外国给予司法协助时，外国往往会要求分得一定得腐败财产，这就导致中国不能全部追回腐败资产，国家利益受到损失，而采取民事诉讼方式则可避免这种情况的发生，中国仅需支付一定的诉讼费用即可；最后，由于判决是由腐败犯罪分子或者腐败财产所在国的法院做出，如果胜诉时，该判决能够得到有效的执行。因此，以民事诉讼的方式追讨海外腐败财产无疑是一项新颖且极具效率的方法。

中国目前流失美国的腐败财产非常庞大，实际上，中国曾在办理中国银行广东省分行开平支行余振东、许超凡、许国俊等人特大贪污挪用案中,为追回被犯罪嫌疑人非法转移到国外的巨额资金,犯罪分子的工作单位——中国银行也曾在美国加利福尼亚等地提起过民事诉讼，冻结并取回了大量涉案财产。但是，相对于中国流失美国的腐败财产总额而言，中国每年成功追回的腐败财产所占的比例仍然较小，中国海外追赃任务仍然艰巨。因此，非常有必要对中国启动国外民事诉讼程序追讨海外腐败财产的法律问题进行深入研究，为今后中国实践部门采取具体的行动提供更多的法律指引。

三、美国法院管辖权概述：联邦法院与州法院

如果决定在美国发起民事诉讼，首先需要解决的是在联邦法院起诉还是在州法院起诉？他们有着怎样的诉讼程序？

众多周知，美国为联邦制国家，存在着两套不同的法院系统，即联邦法院系统和州法院系统，在联邦框架下，美国联邦政府与各州政府，各自均设立了独立的法院系统；同时，各法院适用的民事诉讼规则也不尽相同，一般而言，除了联邦诉讼规则和一些州的民事诉讼立法以外，为了诉讼便捷，每一个法院都有权单独或者联合其它同等级法院颁布仅适用于其自身的本地规则（Local Rules）；另外值得注意的是，由于英美法系传统，在不违背正当程序和法律规定的情况下，法官也可以依据其自身的习惯和经验制定其认为合适的个人操作规则（Individual Practice）。正是由于这些制度的存在，导致美国法院诉讼程序的多样化。一般对于一个美国律所的初级律师而言，在决定起诉之前，必须针对上述内容做一个比较详细的尽职调查。

就美国法院管辖权而言，一般存在着联邦法院管辖权和州法院管辖权之分。对于联邦法院而言，联邦法院属于“有限管辖权法院”（Court of Limited Jurisdiction）,仅就特定事项行使“有限标的管辖权”（Limited Subject Matter Jurisdiction） ,依据28 U.S.C.§1331规定，联邦地区法院依据美国宪法、法律和缔结的条约行使初审管辖权（Original Jurisdiction）。在联邦宪法之下，各州政府在其管辖范围内保留其它所有主权，除专属于联邦法院管辖的事项以外，各州法院基于领土管辖（Territory Jurisdiction）下的所有事项，均可行使管辖权。相对于联邦法院之“有限管辖权法院”，州法院管辖权称为“一般管辖权”（General Jurisdiction）。除非就一定事项，国会立法明确授予联邦法院专属管辖权，否则，即使依据宪法和国会立法联邦法院享有管辖权的案件，州法院也同时具有管辖权，此两种类型的管辖权并存。原告既可选择向合适的联邦法院起诉，也可以选择向合适的州法院起诉。这些案件包括：（1）涉及联邦问题（Federal Question）；（2）涉及跨籍案件。联邦法院享有专属管辖的案件包括“海商案件”、“破产案件”以及“知识产权案

件”等。[1]另外，对于涉及跨籍的案件，当诉讼当事人一方为外国人另一方为一州州民时，联邦法院仍然享有管辖权（Alienage of Jurisdiction）；但是如果诉讼双方都纯粹为外国人时，例如原被告为同一国人时，仅可依据一般管辖权由合适的州法院管辖，由于并无州法院偏袒任何一方之嫌，联邦法院没有管辖权。因此，对于联邦法院和州法院的管辖权，需要判断被告是否有美国国籍或者绿卡。

可见，如果我们决定发起民事诉讼追讨位于美国的腐败资产，则需考虑以下内容：如果被告没有获得美国国籍或绿卡，则仅能选择向其所在的州法院起诉；如果被告已经获得了美国国籍或绿卡，则其所在的州法院和联邦法院对案件都有管辖权。

四、管辖权

在确定到底向联邦法院还是州法院起诉之后，那么下一个问题接踵而至，该具体向哪一个法院起诉呢？

从英美法系角度，对于原告而言，无论原告是否为某国国民，只要他选择在一个法院起诉就表明其同意该州法院做出对其有约束力的判决，愿意接受该州法院的管辖。因此，管辖权的实质问题就是法院基于何种理由对被告行使管辖权。[2]但对于被告管辖权而言，其依据主要有两点：1、依据被告的人身，如果一项争端指向被告人身，基于该争端所形成的管辖权就被称之为“对人管辖权”（In Personam Jurisdiction）,全称In Personam Proceedings Against Individuals,依据此类管辖权所生之判决称为对人判决（A Judgment in Personam）,主要包括能够被告居住在本州岛领域内、法院能够向被告送达传票和起诉状副本等情形；2、针对被告的财产，这类管辖权被称为“对物管辖权”（In Rem Jurisdiction）,全称：Actions in Rem: Proceedings Against Property，该类诉讼指向一项财产利

[1]28 U.S.C.§1332、28 U.S.C.§1333、28 U.S.C.§1334、28 U.S.C.§1338.

[2]参见：王学棉，《美国民事诉讼管辖权探究——兼论对 Personal Jurisdiction 的翻译》，载于《比较法研究》，2012 年第 5 期。

益，一州法院有权解决位于其领域内的涉及利益或者对有形财产或无形财产主张权利的争端，而不管被告是否位于法院地。In Rem Jurisdiction 基于诉讼标的在法院地州所在的司法区这一事实而存在。[3]与对人管辖权不同，对物管辖权不约束被告本身，仅仅用于确定涉案财产的所有权和状态。通常包括土地所有权登记，关于动产或不动产扣押方面等的诉讼,基于这类管辖权所生之判决为对物判决（A Judgment In Rem）。另外，在这两种基础上存在着一种“准对物管辖权”（Quasi-in-rem Jurisdiction）,这类管辖权仅基于被告的财产，而该被告不并在法院管辖权范围内，在这方面和对物管辖权相似，但是根据原告起诉的目的，又分为两种情形，一是针对其它人而主张诉讼标的的完全所有权，二为原告在诉讼开始时申请法院扣押被告的财产，但是其目的仅限于在胜诉以后，可以通过拍卖该财产来偿还自己的债权。对人判决仅对具体的个人的权利产生影响，对物判决则对所有对特定物享有利益的人的权利产生影响，准对物判决则对特定人所享有的特定物的权利产生影响。[4]

综上，我们应区别以下几种情况采取不同的措施：1、如果我们以腐败分子侵犯中国国家或单位的财产权为由，针对被告发起侵权诉讼，则属于对人管辖权，这种方式最便捷高效，但前提是我们能够找到腐败分子的具体位置；2、如果找不到腐败分子的位置，但是能够找到腐败分子转移到美国的腐败资产，则可以直接就此资产提起诉讼，主张返还请求权（restitution claim）,这属于对物管辖权，这种方式需要我们能够追查到腐败财产的位置，如果犯罪分子隐藏的财产位于多处，则需在多地提起多个诉讼；3、在诉讼开始前，申请冻结被告财产以便日后承认和执行，或者针对被告的财产直接主张所有权，这属于准对物管辖权，这种情况下，既需要知道被告的位置也需要知道腐败财产的位置。对于后两种情况而言，提起诉讼的法院均为腐败财产所在地区的法院，比较容易判断。对于第一种情况，则比较复杂，具体确定标准将在下文做重点介绍。

[3]Rose v. Himely, 4 Cranch 241, 277, 2 L.Ed. 608; Overby v. Gordon, 177 U.S. 214, 221—222, 20 S.Ct. 603, 606, 44 L.Ed. 741.
[4]Hanson v. Denckla：357 U.S. 235, 78 S.Ct. 1228U.S. (1958).

五、确定对人管辖权的标准——最低限度联系（Minimum Contacts）

英美法系国家关于对人管辖权的依据是最低限度联系标准。在理论上，人们习惯地将最低限度联系原则称为“长臂管辖权”（Long Arm Jurisdiction）理论。美国关于最低限度联系的规则主要体现在大量判例中：

在Pennoyer案中，美国联邦最高法院指出，法律的正当程序是指，在进行司法程序中，保护和执行私人权利的一整套法律流程。为了赋予这套程序的合法性，首先法院必须有权审理该诉讼标的，如果该诉讼标的仅仅在于决定被告的个人权利，那么该被告必须在法院的管辖范围内在本州岛被送达，或者他自愿出庭应诉。[5]在这里最高法院确定一州法院获得对外州被告属人管辖权的两个标准：1、被告在其管辖范围内在本州内被送达；2、被告自愿出庭应诉。另外，对于送达的方式，最高法院认为采用公告送达等替代性送达方式取得对被告的管辖权是无效的，因此只能通过直接送达被告本人的方式取得管辖权。

在随后的几个判例中，美国最高法院对最低限度联系进行了发展。在International Shoe Co案中，法院认为确定所谓“最低限度联系”主要取决于两点：1、被告是否在法院地从事系统的和连续性的商业活动;2、针对被告的诉因是否源于这些商业活动。至于被告是否在法院地实际出现,则无关紧要。[6]

到了上世纪80年代,最低限度联系原则又得到进一步发展。1980年World-Wide Volkswagen Corp. v. Woodson（国际大众公司诉伍德森案）中, 联邦最高法院将所谓的“有意利用”(purposeful availment)标准加入到作为判定“最低限度联系”的一个基本标准:即被告为自己的利益有意利用法院地的商业或其它条件。[7]

5 Pennoyer v. Neff, 95 U.S. 714, 24L.Ed. 565(1878).

6 同上

7 Word-Wide Volkswangen Corp. V. Woodson, 444U.S. 268, 100S .Ct. 559, 62 L. Ed. 2d 490(1980).

综上，在长期的司法实践中，美国联邦最高法院就如何适用“最低联系”得出了四个准则：1、被告在某一州的活动是持续而系统的、且起诉因发生于该州，则属该州管辖；2、被告在一州仅从事零星的或偶然的活动或单独孤立的行为，且诉讼也与这些行为无关，则不属该州管辖；3、即使诉讼原因与被告在当地的行为无关，但其在当地持续的活动具有某种性质最终使该州获得管辖权；4、被告在当地零星甚至单一的活动引起了诉讼，在特定的情况下该州具有管辖权。[8]在具体司法实践中，第1和第3种情形也被称为一般对人管辖权（General personal jurisdiction），第4种情形被称为特对人殊管辖权（Special personal jurisdiction）。为行使一般属人管辖权, 法院必须决定被告与法院地是否具有充分、系统和持续的联系，以支持一个合理的行使管辖权的理由；[9]在具体案件中，还需考虑：1、被告出庭和举证的负担；2、法院地的利益；3、原告获得救济的利益；4、其他州的利益，等。为行使特殊属人管辖权, 法院必须考查：被告、法院地和诉讼之间的联系，以决定维持诉讼是否违背传统公平参与和实质正义的观念；[10]法院必须考虑：1、被告在法院地活动的质量、性质和程度；2、行为结果发生在法院地的可预见性；3、被告、法院地与诉讼之间联系与诉因之间具有直接的关系。[11]法院对于这些因素的考查具有非常大的自由裁量权。

综上，如果我们决定针对腐败犯罪分子提起侵权之诉，则需要细致考察犯罪分子藏匿的居住地、转移腐败资产的行为地、挥霍腐败资产的行为地等诸多因素，上述地点法院均可能受理案件。

---

[8] 参见：杰克·H•佛兰德泰尔 等 著， 夏登俊等译，《民事诉讼法》，北京：中国政法大学出版社 2003 年版，第 112 页。

[9] Stuart v. Spademan, 772 F.2d 1185, 1191 (1985) (citing Keeton v. Hustler Magazine Inc., 465 U.S. 770, 777-81, 104 S.Ct. 1473, 1480-81, 79 L.Ed.2d 790 (1984));

[10] Southmark Corp. v. Life Investors, Inc., 851 F.2d 763, 772 (1988).

[11] Hydrokinetics, Inc. v. Alaska Mechanical, Inc., 700 F.2d 1026, 1028 (1983).

六、总结

海外犯罪分子实为民族之贼，国家之敌，首要目标仍然将其引渡回国，让其接受审判和惩罚。同时，我们也要考虑怎样将腐败资产追讨回来，减少国家和单位的损失，即便最终不能将其成功引渡回国，如果能够将其所有腐败资产追讨回国，断其追求腐化生活的经济基础，这对其也是一种震慑，相关的劝返工作也会更加顺利。

在美国提起民事诉讼，依据美国法律，一般而言，腐败财产所在地法院享有对物、准对物管辖权，而腐败分子藏匿之地、转移腐败资产之地、挥霍腐败资产之地等法院享有对人管辖权，如果腐败分子已经加入美国国籍或者取得美国绿卡，则上述地的州法院拥有管辖权，如果腐败分子没有加入美国国籍或者取得美国绿卡，则上述地的州法院和联邦法院都有管辖权。

以民事诉讼方式直接针对腐败犯罪分子或者腐败财产提起诉讼，这只是诸多追讨海外腐败资产方式的一种，如果其他方式均难以取得进展时，也许这种方式会给反腐败调查人员带来新的工作思路，对于全球各国的反腐败工作，也具有重大的借鉴和促进意义。对于各国律师等法律工作者来说，这也不失为其增加社会影响力、扩展业务的有效方式之一。

参考文献：

Hanson v. Denckla；357 U.S. 235, 78 S.Ct. 1228U.S.

Hydrokinetics, Inc. v. Alaska Mechanical, Inc., 700 F.2d 1026, 1028.

Overby v. Gordon, 177 U.S. 214, 221—222, 20 S.Ct. 603, 606, 44 L.Ed. 741.

Pennoyer v. Neff, 95 U.S. 714, 24L.Ed. 565.

Rose v. Himely, 4 Cranch 241, 277, 2 L.Ed. 608.

Southmark Corp. v. Life Investors, Inc., 851 F.2d 763, 772.

Stuart v. Spademan, 772 F.2d 1185, 1191.

Word-Wide Volkswangen Corp. V. Woodson, 444U.S. 268, 100S .Ct. 559, 62 L. Ed. 2d 490.

杰克•H•佛兰德泰尔 等著，夏登俊等译，《民事诉讼法》，北京：中国政法大学出版社2003年。

王学棉，《美国民事诉讼管辖权探究——兼论对 Personal Jurisdiction 的翻译》，《比较法研究》，2012年第5期。

Available online at jls.pruna.eu
Journal of Legal Studies
Journal of Legal Studies, 2016, 74–79
Received: 19 May 2016. Accepted: 8 June 2016. Published: 2 August 2016

“Availability of credit and secured transactions in a time of crisis”书评

李大朋♣

“Availability of Credit and Secured Transactions in a Time of Crisis”一书为论文集，由英国剑桥大学出版社（Cambridge University Press）于2013年12月12日出版，全书共320页。该书由英国杜伦大学法学院高级讲师N. Orkun Akseli主编，Sir Roy Goode作序，共收录了来自全球优秀学者的十三篇学术论文。本书从一个广泛的视角选择相关论文，包括：银行在经济发展和金融危机中的作用，贷款便利化及其政治与政策视角，国际金融机构的地位，国际组织的参与及其对法律和市场的影响，从国内法角度谈英格兰担保交易法律改革，等等。

该书第一部分标题为贷款的可获得性，包括三篇文章，分别是David Bholat, Money, Bank debt and business cycles: between economic development and financial crisis; Gerard McCormack, Secured transaction law reform, UNITRAL and Export of foreign legal Models; Joanna Gray, Commentary on availability of credit.

♣中国政法大学，法学博士。主要研究方向：国际法学。E-mail: dapengli1989@163.com

该部分集中于贷款的可获得性、获得贷款的挑战以及采用一套自由化模式来统一和改革法律所带来的问题。在第一篇文章中，作者首先考察了在历史与经济理论上银行所发挥的作用，其次作者辨析了有银行和无银行时经济增长和经济发展的区别，信贷增加是一把双刃剑，既可能引发繁荣，也可能导致金融危机，作者指出引发现在这场危机的消费信贷和与此对应的家庭债务恰恰是由于全球储蓄过量（global savings glut）而引起的，亚洲经济大量的储蓄通过银行进入全球大宗商品市场，使得利率被压低并在资本输入国增加了大量的金融投资，进而导致消费信贷和家庭债务的扩张，最终引发经济危机。不管这一理论是否正确，这都意味着目前国内政策缺乏清晰度，不足以支撑资本自由化。因此，作者倾向于将银行描述为在金融危机的产生中的具有独特性的充满问题的机构（uniquely problematic institution）。最后，作者对于银行在经济发展中发挥的积极作用抱以强烈的怀疑，并建议以其他机制取代其在金融中的核心地位。从本书的目的来看，这些其他机制就包括融资担保制度。在第二篇文章中，作者对于目前UNCITRAL指南中所寻求的自由化进行了批评，表明担保交易法律改革的现代化并不等于自由化，应当受制于更严格的监管。第三篇文章为前两篇的评论，故在此不叙述。

第二部分标题为Involvement of international financial institutions in secured transaction law reform, 主要包括四篇文章，与第一部分相同，最后一篇文章为前三篇的评述，分别为：Terence C. Halliday, International Organization as global lawmakers: seven shifts in practice for secured transactions law and beyond; Spyridon V. Bazinas, The creation of interntaional commercial law standard by interntaional fiancial institutions: why they do it and when they should; Frederique Dahan, The power of secured transactions law and the chanllenge of its reform; Loukas Mistelis, Commetary on the invlovment of international financial institutions in secured transaction law reform. 在第一篇文章中，作者通过分析国际组织制定的标准对市场的影响，进而分析这些国际组织如何制定标准，在此基础上，提出七个改进意见：由隐形的国际金融机构立法走向显性的国际组织立法、从单纯的发展主义走向灵活的发展主义、从未验证过的理论走向已经验证的理论、从单一的模式走向可选择的模式、从狭窄的研究走向宽泛的交叉研究、从全球化的地区主义（globalized localism）走向统一的标准、从

静止性规范走向递进式推动（文章的意思是：法律理论与法律制度相协调）。第二篇文章，作者列举分析了国际立法机构与国际金融机构在制定国际担保交易法律标准时的重叠，作者建议国际金融机构应当与国际立法机构合作，以继续推进其在经济发展中的职责。第三篇文章在于阐述欧洲重建与发展银行（European Bank for Reconstruction and Development）在担保交易改革中基本信念：担保交易法便利化的目标应当基于法律的高效率，担保交易法多功能，因此担保交易改革也应当拥抱这一多功能性，担保交易法改革并未失去势头。综上，本部分主要讨论国际金融机构和国际组织在新兴经济体和贷款便利化过程中，在制定担保交易标准时所具有的地位以及其利益关注点。

本书的第三部分主要探讨联合国贸易法委员会关于担保交易的立法指南以及联合国国际贸易应收账款转让公约，分别为：Spyridon V. Bazinas, The utility and efficacy of the UNITRAL Legislative Guide on Secured Transaction; N. Orkun Akseli, The utility and efficacy of the UN Convention on the Assignment of Receivables and the Facilitation of the Credit; Henry Deeb Gabriel, Commentary on the availability of Credit and the Utility and efficacy of UNCITRAL's legislative efforts in secured transaction. 这两份文本及其基本原则为立法者在担保交易立法改革中提供了有价值的工具。第一篇文章深度地探讨了该指南在减少贷款成本中作用，考察了指南的核心政策。第二篇文章探讨了联合国国际贸易应收账款转让公约的基本原则，他指出现代化的高效的可背书应收账款融资规则对于减少贷款成本具有重要意义，在经济危机中能够有效地减少现金流需求，促进投资，这些规则可被作为国内法改革的起点。第三篇论文主要集中于讨论指南的"软法"性质，以及从反面论述对于应收账款公约失望的几点理由。

第四部分探讨由国际机构和国际金融组织制定的国际标准能否以及在多大程度上有利于改革信贷和担保法律,分别为：Anjanette H. Raymond，How many international standards assist law reform in England? Noel Macgrath, Commentary on the international standards and the reform of England personal property security law; Hugh Beale, The UNCITRAL Legislative Guide on Secured Transaction as a model for law reform: some

conclusions. 对于英国来说，目前已经达成共识的是，为了克服经济危机，除应该在银行业进行改革外，担保法律改革业已刻不容缓，以便企业能够更便利地得到融资。第一篇文章认为英国应当彻底改革其动产财产担保法律，而第二篇文章持一个相反的立场，认为可以通过持续的方式改革其动产财产担保法律。第三篇作为一个总结，指出国际贸易法委员会关于担保制度的指南可以使得担保交易法律体系更有效率。

担保交易在扩大融资途径，构建一国健康的金融体系中发挥着重要的作用。例如，多年来，世界银行很多研究报告均表明在不允许对于动产设置非占有性担保的发展中国家，其经济发展面临着非常严重的障碍。因此，很多国际机构，包括世界银行本身、欧洲重建和发展银行、联合国国际贸易法委员会(UNCITRAL)、国际私法统一学会(Unidroit)等，均在寻求鼓励各国颁布担保交易法的努力，借此可以鼓励银行和其他金融机构扩大贷款额度，以促进经济的发展 (Akseli 2013, p. xi)，这对于走出全球经济危机发挥着重要的作用。

但是，另一方面，担保交易法律制度改革实属不易。自上世纪七十年代开始，基于担保交易法律的统一现代化能够有效地降低贷款成本这一认识，国际立法机构和金融机构制定了大量的与担保交易法律有关国际条约和法律文件，希望借此改革担保信贷法律。彼时，担保法律制度仅为国内法范畴，与财产法、合同法和破产法有着密切的联系，这些法律反映了不同国家在文化立场和公共政策的不同偏向。但是数年来，这些不同偏向，加之各国不同的政治和经济目标、不同法律体系之间的竞争、国际法产生过程中的矛盾以及法律从业者对于新规则的评价与适用等因素，已经使得一个可以适应金融市场全球化的担保交易法律的改革无法进行。

必须知道，法律为社会变迁之引擎(Wacks 2006, p. xii)。若一个国家的社会组织结构、经济和竞争力量由于全球金融危机和担保信贷的缺位而改变时，实现担保信贷法律的现代化就是至关重要的了。获得担保的能力不仅影响贷款成本，在一些场合甚至决定最终能否获得贷款，无论在发达国家还是新兴国家，由于金融危机，低效率的担保信贷法律所导致的

困难正越来越严重。商业对于法律有期望，国家也有责任建立金融和法律框架以消除融资障碍。通常认为，旨在提供可预测性并使之现代化的有关担保交易法的国际文件发挥了积极的作用，并且影响了相关国内法律改革。

因此，本书旨在讨论由于各国无效率的担保贷款法律而引起的严峻挑战，以及为了克服这些挑战，对建立在国际金融机构和国际立法机构制定的担保交易国际法律标准基础上的法律改革进行探讨，尤其是联合国国际贸易应收账款转让公约（UN Convention on the Assignment of Receivables in International Trade）和联合国贸易法委员会关于担保交易的立法指南（UNCITRAL Legislative Guide on Secured Transactions），以及其他由世界银行和欧洲重建和发展银行发起的全球担保交易统一化与现代化运动。

综上，通过本书，我们可以得到以下启示：

1、对于银行业松弛的监管是导致全球金融危机的罪魁祸首，因此应该进一步加强对于银行业的监管。对于担保制度进行改革，是加强银行业监管的方式之一。

2、担保能够有效较低贷款成本，而增加贷款额度，减少信贷成本能够有效地刺激全球经济的发展。健全的担保交易法律能够给相关国家带来巨大的经济利益，吸引信贷，促进企业的成长，扩大贸易。为得到这种目标，担保交易法律必须高效，包括高效的司法和破产系统等，因此改革当前的担保法律就显得尤为重要了。

3、在各国经济尚未走出全球金融危机的阴影之前，目前金融交易相关的法律并不能满足金融市场全球化的要求，尤其是在法律的确定性方面。不同的法律传统、经济和政治考量均影响着当前担保交易法律的制定和实施，因此应当尽量协调这些分歧，而由国际组织和国际金融机构制定的担保交易文件，即通过软法的效果，也许能够解决这一问题，其功能与美国的《统一商法典》等如出一辙。

4、改革当前国内担保立法的途径大概有两种，第一种是直接借鉴有关国际组织和国际金融机构的有关文件，并将其精神贯穿到本国立法改革之中，另一种就是借鉴各国成功的经验，将其成功的经验引入到本国的担保改革立法中去。本书集中于前一种方式，国际组织和相关国际金融机构的地位与作用。

综上，本书从动产担保，以及基于动产担保的贷款制度改革角度，谈经济危机的预防与克服，观点新颖，令人深思。

参考文献:

Akseli, N. O. 2013. Availability of Credit and Secured Transactions in a Time of Crisis. Cambridge University Press.

Wacks, R. 2006. Philosophy of Law: A very Short Introduction. Oxford University Press.

Nordic Journals

Available online at www.nordicjurnals.eu/nj
Journal of Legal Studies
Journal of Legal Studies, 2016, 80–91

Journal of Legal Studies

Received: 21 August 2016. Accepted: 5 October 2016. Published: 22 November 2016

Workers' Right of Living Space Under the Background of Global Capital: The Example of Dormitory Regime of Foxconn

Xiang Li♣

Abstract: For workers at the end of global supply chain, moving to dormitories provided by employers implies subordinates their living space to the open surveillance of employers in Foucaultian sense. This paper constructs workers' right of space to protect workers being away from employers' interference in their living space. This right is derived from current Civil Law and Constitutional Law. It also relies on the citizenship theory of T. H. Marshall. Additionally, this right is also designed to countervail workers' "triple" dependence on employers. After analysing two reasons why workers' right of space is compressed, this paper analyses workers' countermovement of defending their right by adopting "double movement" theory of Karl Polanyi. Finally, the solutions to solve this problem are explored in this paper.

Keywords: Global capital; Workers; The right of space; Dormitory regime

The research on the right of space comes from two topics. Firstly, it is from the research on dormitory regime discussed by scholars, such as Pun and

♣ Ph.D student of Leiden Law School, Leiden University, The Netherland.
x.li@law.leidenuniv.nl

Smith (Pun and Smith, 2007; Smith, 2003). They argue that dormitories are place where labour control and labour struggle can be produced. Secondly, it comes from the research on the housing problem in urbanisation. It is generally agreed that housing resources should be enjoyed by migrant workers. Nevertheless, the research from legal perspective on this topic is missing from previous research. This paper tries to fulfill this gap. It constructs the right of space, retrospects its legal sources, investigates why this right is compressed, and then puts forward suggestions to solve the problems.

The proposal of question

On February, 2nd, 2015, Guo, Jun, an important official of All-China Confederation of Trade Unions (ACFTU) criticised enterprises like Foxconn. He commented that illegal overtime working happened in these enterprises resulted in workers' various mental problems, sometimes even caused workers' suicides or death. Foxconn rejected that there were cause-and-effect relations between overtime work and suicide. In the verbal conflicts between Foxconn and ACFTU, one fact admitted by both was that overtime work does exist in Foxconn. Currently, the regular statutory working hour of China is 40 hours per week. Overtime working per month should not be longer than 36 hours. However, according to the report of Fair Labour Association (FLA), in November and December of 2011, there were respectively 34% and 46% of Foxconn workers worked more than 70 hours per week.[1] This data indicates that the working hour system of Foxconn violates the statutory standard on working hours. In other word, Foxconn invades workers' resting rights.

However, the statutory labour standards on working hours are far from able to explain the overtime work at Foxconn. The practice of any rights has to rely on two dimensions: time and space. The infringement of Foxconn on

* Ph.D student of Leiden Law School, Leiden University, The Netherlands. E-mail: x.li@law.leidenuniv.nl

1. See Fair Labor Association, *Foxconn Investigation Report,* 2012, http://www.fairlabor.org/report/foxconn-investigation-report, Accessed on September 1, 2016.

workers' resting rights is at the premise that workers are available in the dimensions of time as well space. The space of dormitories facilitates Foxconn to force workers to do overtime work. Dormitories at Foxconn are arranged according the gender of workers. Only workers with same gender can be arranged into a dormitory. Thus these dormitories are incompatible with workers' family life. It means that these dormitories can only maintain short-term industrial relations. Foxconn' bahaviour of making use of dormitories to compress workers' resting alludes to the right of space and resting of workers. The right of resting has already been regulated in current legislation. However, the right of space of workers has not been defined. Thus, this paper pays more attention to this right.

The legal sources of the right of space of workers

The right of space of workers is an abstract right which has not been defined yet. It is a right regarding on workers' living space. It is characterised by exempting from employers' interference in living space. Although it is a new right, the sources can be found from current laws or legal thoughts**.**

Sources in Property Law and Constitution

Although dormitories are owned by employers, they are also living space of workers. Workers lawfully enjoy the right of temporarily possessing the living space. This means that production orders from employers shall not entered into the living space of workers. In addition, workers' right of resting is clearly regulated by Article 43 of *Constitution*. The space for workers to realise their rights of resting is in general incompatible with the space where workers fulfill the duty of work, especially in labour- intensive industries. Dormitories, regardless that they are inside or outside of factories, should guarantee workers' right of resting firstly. As such, the source for this right can be found both in *Property Law* and *Constitution.*

The citizenship theory of T. H. Marshall

According to the citizenship theory of T. H. Marshall, citizenship comprises of rights on three elements: civil rights, political rights and social rights (Marshall, 1950, p.10-11).The civil rights refer to the freedom of person,

speech, religion, property, and the right to conduct contract. Political rights mean the rights to participate in political power. Social rights include the right of enjoying economic welfare and security to live a life of a civilised human being. Housing problem belongs to the social elements of citizenship according to Marshall. He argues that the equality hiding behind citizenship could mitigate the inequality of social class, though only to a limited degree. He expects the formal equality in empowerment to correct the inequality in social class. He also admits that absolute equality is impossible. Rights can be unevenly granted, but it is difficult to control the implementation of rights. It is restricted by factors such as wealth, education background of the rights of subject.

It is undoubtful that the lack of social welfare contributes to workers' dependence on low salary provided by enterprises. However, the absence in empowerment is a main factor leading imbalanced labour relations in China (Li, 2012). Even if migrant workers are empowered equally, they do not have the advantage to realise their rights. The implementation of social rights in citizenship relies on the economic conditions of the subjects of the rights. In general, Foxconn workers earn less than workers who have decent jobs. This is due to that the majority of Foxconn workers are made of migrant workers. The difference in wealth dooms that Foxconn workers can not realise their right of housing. Dormitories inside factories provided by employers could save their cost of housing and transportation. Nevertheless, the freedom of person is a passive right. It can be realised without the conduct of others. The practice of this freedom is not restricted by the wealthy situation. Dormitories are provided by the capital. Workers temporarily enjoy the right to occupy it. Living in dormitories does not mean that workers give up their freedom of liberty in dormitories. Workers shall not be managed in their living space provided that they do not cause troubles to the property of their employers. The order of production should also be away from the living space of workers.

The necessity to overcome the triple subordination of workers to employers

Workers who lived in dormitories provided by employers are subordinated to employers at three aspects. The classical 'double subordinations' is

challenged by the dormitory regime. Apart from subordination to employers from the perspective of personality and economy, workers also rely on employers on living space. The availability of their living space is constrained by the term of their labour contract with employers. The low salary of workers makes it less possible for workers to rent houses outside factories. Thus, workers have to subordinate themselves to the management of employers in living space. To overcome workers' triple subordination to employers, it is necessary to design the right of space of workers.

Reasons for the compression of the right of space of workers

The encroachment of the right of space of is not unusual to see. Workers are easily required by employers to move to workshop from dormitories when there are urgent tasks. This section gives two reasons of the encroachment.

Asymmetric free market economy

Globalisation relies on the free movement of capital and other production materials. Governments play important roles in guiding the capital and labour entering into market. Governments' enthusiasm towards foreign capital is more or less epidemic in developing countries. In general, local governments in developing countries compete for attracting investment to locate in their jurisdiction. The competition of 'the race to bottom' among local governments on labour standards and other thresholds facilitates the entry of foreign capital into China.

There are not too many obstacles preventing the relocation of Foxconn from coastal area to inland of China. Local governments are busy with supplying Foxconn with various benefits instead of doubting whether the relocation will exploit cheap labour at their jurisdiction or not. The monopolistic position of Foxconn in market has been achieved by the alliance between local governments and Foxconn (Pun and Xu, 2012, p. 50).However, migrant workers are not granted with benefits when they enter into market economy. They cannot enjoy housing, medical and education resources as urban citizens. They even cannot afford the rent of cheapest house in cities. Dormitories inside factories supply them with space to locate in urban areas. Thus, they have to subordinate themselves under the control of employers.

Nevertheless, Foxconn is only an enterprise. It can not bear as many functions as a society. It can do little in supplying workers with living space. In Long Hua and Guan Lan industrial parks of Foxconn, 400,000 workers reside in a place less than 3-square kilometres. The impotent role of local governments in guiding workers to enter into market economy facilitates the infringement of Foxconn upon the right of space of workers. This is inevitable when workers choose dormitories of factories as their living space.

Shortened living-working space

Under the background of free movement of capital, dormitory regime not only supplies the capital with cheap labour cost, but also provides them with the flexible labour. The change of production model from Taylorism to flexible demands casts a challenge to the supply of labour. It requires that labour must be available whenever there are production tasks. It also requires that labour must be able to move to working place as quickly as possible when there is urgent production order. The distance from working place to living space of workers could even change the fate of enterprises like Foxconn.

Companies like Foxconn are at the end of global supply chain. Establishing a timely delivered system of goods are very vital for them to attract clients. Otherwise, they may lose their clients. In the supply chain of Apple, foundaries are always in the disadvantage position compared to their clients. The gap was observed in the cooperation between Apple and Foxconn. Apple ever subcontracted the bills to Pegatron, another foundary. This pushes Foxconn to a more disadvantage position. Therefore, it has to minimise the distance from working space to living space of workers to keep being competitive in global supply chain.

For labour-intensive factories like Foxconn, the workplace of workers is workshop. Dormitories are the living space of workers. The distinguished characteristic for these dormitories is that they are managed as workshops. The capital manages and controls workers in dormitories as they did in workshops. Thus, dormitories, which are supposed to be the resting and comfortable place for workers, are changed into the extension of workshops

(Pun, 2011, p.37). The influence of enterprise managements cannot be avoided in dormitories. Dormitory regime places workers under the "the open space" in Foucault sense. This could re-shape workers' life (Pun and Ren, 2006, p.133). In other word, workers living in dormitories supplied by employers are consistently in the state of on-call of production order. Thus, they are required to be available at any time. As such, the shortened working-living space of workers reinforces the possibility to infringement upon the right of space of workers.

The countermovement of workers defending their right of space

The shortened space of working-living of workers makes it possible to compress the right of space of workers. Based on the theory of Polanyi (2007, p.2), "A self-adjusting market implied a stark Utopia. Such an institution could not exist for any length of time without annihilating the human and natural substance of society; it would have physically destroyed man and transformed his surroundings into a wilderness". Polanyi (2007, p.44) argues that double movements existed in 19th century: the extension of market organsiation, and the movement restricting the former movement. The extension of market organsiation relies on deregulated policies and free trade. The second movement are embodied at the protection of land, labour, working class, etc.

However, Polanyi only provides us with a signpost of anti-hegemony. He neglects the roles of politics in countermovement. He supposes that the social resistance mixes with the concession of class. Friedman (2014, p. 18-22) divides the countermovement in China as two intertwined moments (insurgent moment and institutional moment). Institutional moment deals with the decommodification in economy and the integration of working class in politics. Insurgence moment refers to the process that marginalised group engaged in disorganized and temporary resistance to commodification. The countermovement started rather late in China. Currently, it mainly stays at the period of insurgence moment. Where there is oppression, there is protest. For workers at the end of global supply chain, the commodification of their labour has already spread to their living space. It is destined that their countermovement against commodification will happen.

On 23rd-24th, September of 2012, the riot happened in Foxconn branches of Taiyuan attracted the attention of media inside and outside of China. More than 2,000 workers participated in this event and 40 of them were injured. The trigger of this riot was the conflict between several workers and the security guard. These workers failed to show their ID card when they entered into the dormitory. They were dragged into a van and beaten by the guards. Then it deteriorated to a group fight. [2]

This riot did not directly bring better treatment to workers. Neither it caused changes to enterprises or the country. However, it proves that migrant workers have already woken up. They are protesting the violation of their right of space. This riot also evidences the analysis of Friedman on two intertwined movement moments (2013 and 2014). Compared to the infringement happened in workplace, the violation happened in living space is more likely to irritate workers. The right of space of workers deal with human dignity. Thus, the discontent emotion of workers can be easily ignited when their dignity is ravaged.

The solutions of preventing the violation of the right of space of workers

As stated before, local governments' conflicting attitudes in guiding the capital and workers into market economy contributes to the infringement of the capital on the right of space of workers. The shortened distance of working-living strengthens the possibility of the infringement. This resulted in the countermovement of workers to safeguard their rights. However, the countermovement has not brought the durable integration of the working class at the political level. In order to fundamentally prevent employers from violating this right, it is necessary to protect this right. Currently, it is impossible to create a special law on this abstract right. The following are several suggestions which might be conducive to solve this problem.

[2] For more details about this report, see Foxconn's Factory, Producing iPhone 5's, Erupts in a Riot, China Labour Watch.

The equal empowerment of housing

The equal right on housing is a right that civil society should guarantee. It requires that workers equally have this right, but also entails the equal possibility to realise this right. China is heading for this direction. Central government has promulgated several documents to protect this right. Since 2011, central government has begun to encourage to establish public rental houses where are crowded by factories. Public rental house is compatible for workers' family life. Thus it is conducive to maintain long-term labour relations. Additionally, it could also reduce the dependence of workers on employers. Thus, workers can be free from the management of employers at their living space. The production efficiency can also be guaranteed since public rental house are usually closed to factories.

Protecting workers' collective labour rights

Collective labour rights of workers include the freedom of association, the right of collective bargaining and the right of strike. Collective bargaining is at the centre of three collective labour rights. It is at the premise of the freedom of association, and guaranteed by the right of strike. There are "two subordinations" in individual labour relations. Thus, workers are easily placed to a disadvantage position in individual bargaining. Through grouping workers' individual power, collective bargaining can overcome the weakness of the two subordinations. Workers' rights and interests are more likely to be achieved in collective bargaining than in individual bargaining. Collective bargaining could also supply workers and capital with an effective and peaceful mechanism to solve labour disputes. Currently, the right awareness of workers has increased. If legislation could not provide workers with an effective way to voice their demands, workers may probably choose wildcat strikes to address their grievance. Collective bargaining is a long-term strategy to maintain industrial peace. It is also an approach to save legislative cost, since it allows flexibility across industries in creating labour standards. Hence, the collective labour rights of workers should be protected. It can contribute to prevent employers from violating workers' individual right, such as the right of space.

Changing the attitudes of local governments

In China, many pro-labour policies from central governments are more or less undermined when they arrive at local level. There is divergence between local governments and central government. Central government gives priority to social security. However, local governments put on emphasis on local economic growth. Given this difference, it is reasonable to conclude that even if central government is intentioned to ameliorate working conditions, it is hardly to be realised (Bai, 2011, p. 25). The overlapped interests between local governments and housing developers is the main obstacle that preventing workers to realise their right of housing. The housing problem directly relates to the living of workers. If this problem can not be handled properly, it can bring instable factors to the society. Dormitories only provide workers with basic room of surviving. The limited living space can reinforce the discontent of workers towards their employers. Riots or group fight might occur under this circumstance. The unorganised movement may negatively affect local economy and break the images of local governments if they are not handled properly. Thus, local governments shall handle the housing problems of workers properly.

Legislation on collective labour relations not only influences economic development, it can also impact the stability of the country. However, impractical legislation in this field may not supply workers with effective mechanisms to address their demands, but bring in a wave of strike. Thus, regulating collective labour rights at national level should be cautious. This is due to that labour movement develops unevenly in China. However, it is much easier to make a practical law at local level than at national level. Local governments can create local regulations in this aspect by exercising their decentralised economic and legislative power. Local governments can achieve industrial harmony through regulating workers' collective actions and provide feasible laws on collective bargaining. This has already shown up in some coastal areas like Guangdong. Through local regulations, it is possible for local government to contain labour movement into reasonable and rational way. Thus, local governments should appropriately exercise their administrative power and create practical local regulations in this field.

Conclusions

Housing problems are main obstacles for workers to get involved in market under the background of globalisation. The dormitories provided by the capital supply workers with basic living space for surviving. However, the appearance of dormitories saves the cost of employers to hire workers. Additionally, it also facilitates the capital with the convenience to disturb workers. The right of space of workers are designed to balance the triple subordination of workers to employers. This right is also an embodiment of the Citizenship theory of T. H. Marshall. This right is characterised as being free from the interference of employers in living space. Currently, this right is violated on two reasons. Firstly, local governments are biased on employers in guiding the capital and workers into market economy. Secondly, the distance of working-living is shortened. The encroachment of this rights triggers workers' countermovement. However, labour movement has not brought the change at national level. To fundamentally solve this problem, it is imperative to change legislation. It can be solved by equal empowerment on the right of housing, legislating collective labour rights, and altering local governments' attitudes.

References

Bai, Ruixue. 2011. The role of the All-China Federation of Trade Unions: implications for

Chineseworkers today, *Working in USA*, Vol. 14, pp. 19-39.

Friedman, Eli. 2013. Insurgency and institutionalization: the Polanyian countermovement and Chinese labor politics, *Theor. Soc.,* Vol. 42, pp. 295-327.

Friedman, Eli.2014. *Insurgency Trap, Labor Politics in Post-socialist China*, Ithaca: ILR Press.

Li, Yaxiong.2012.Research on the labour-*capital relations in foundries*-based on the analysis of Foxconn, *Research of Socialism*,Vol. 1, pp. 110-113.

Marshall, Thomas Humphrey.1950. *Citizenship and social class and other essays*. London: CUP.

Polanyi, Karl. 2007. *The Great Transformation: the political and economic origins of our time.* Boston: Beacon Press.

Pun, Ngai and Smith, Chris. 2007. Putting transnational labour process in its place: the dormitory labour regime in post-socialist China. *Work, Employment and Society*, Vol. 21(1), pp. 27-45.

Pun, Ngai. 2011. Living space: prisoned in the foundry of Foxconn, *Chinese workers*，Vol.3, pp. 36-40.

Pun, Ngai, and Xu, Yi. 2012. Monopolistic capital and Chinese workers-taking the system in Foxconn as an example, *Cultural Review*. Vol. 02, pp. 48-54.

Ren, Yan and Pun, Ngai. 2006. The labour system of dormitories: The difference space of labour control and struggle, *Open times*, Vol. 03, pp. 124-134.

Smith, Chris. 2003. Living at work: management control and the dormitory labour system in China, *Asia Pacific Journal of Management*, Vol. 20, pp.333-358.