Social Sciences in China
Vol. XXXII, No. 1, February 2011, 66-79

Cyber Variants of Traditional Crimes and Criminal Law Responses

Yu Zhigang

College of Criminal Justice, China University of Political Science and Law

传统犯罪网络变异的原因是多方面的，直接诱因是网络空间的技术性代际差异；传统犯罪的网络变异表现为犯罪构成要件要素的变异、社会危害性的变异和犯罪形态的变异三个方面。扩张化的司法解释是解决这一问题的首要选择，但其局限性也是明显的；面对网络空间中传统犯罪的变异态势，将部分预备行为提升、独立化为实行行为，将部分共犯行为加以正犯化，将会是未来刑事立法无法回避的两个选择。

关键词：网络犯罪　传统犯罪　社会危害性　刑事立法　变异

The reasons for cyber variants of traditional crimes are many. A direct catalyst is the generation gap caused by the transition from Web 1.0 to Web 2.0. Such variation takes the following three forms: variation in the elements constituting a crime, in the social harm done and in the form of the crime. Expansion of judicial interpretation is the primary choice for handling cybercrime. However, its limitations are also obvious. In the face of cyber variants of traditional crimes, we argue that raising the status of some acts of preparation to that of independent acts of execution and making some joint offenders into principal offenders offers two important solutions that can no longer be avoided by China's criminal law legislation.

Key words: cybercrime, traditional types of crime, social harm, criminal law legislation, variation

In the information age, cyber variants of traditional crimes have become one of the most complex issues in criminal law theory and in legislation and criminal justice.

I. Background Analysis of Cyber Variants of Traditional Crimes

In the course of the transition from Web 1.0 to Web 2.0 and from media as information to media as "life platform," cyberspace has given rise to a technological generation gap that has

ISSN 0252-9203

DOI: 10.1080/02529203.2011.548919
http://www.informaworld.com

become a powerful force shaping cyber variants of traditional crimes.

1. The force boosting cyber variants of traditional crimes: two important stages in the evolution of the Internet

The underlying reason for cyber variants of traditional crimes is the virtual nature of the Internet, but its most direct booster and incentive is from the two great changes in the evolution of the Internet. The first of these is the transition from the virtual world to the real world. The virtual nature of the Internet is becoming increasingly relative; online behavior is ceasing to be purely virtual and is acquiring more and more social significance. Internet users have to take legal responsibility for what they say and do online. At the same time, the great social and economic value of the Internet not only acts as a catalyst for every kind of illegal or criminal online activity but is also the target of such activity. The second change is the shift from a medium designed to provide pure information to a "life platform." In its early history, the Internet emphasized the connections afforded by the "net;" now, it emphasizes the "inter" of its title, i.e. interdependence. The Internet has gradually expanded from being a tool for the dissemination of pure information to its current role in various commercial areas and from providing entertainment and information services to being a "life platform."

2. Background to cyber variations of traditional crimes: the transition from "net connections" to "interdependence"

The transition from "net connections" to "interdependence" has contributed to two important changes to cybercrime. (1) Crime characterized by one-on-one online interaction is becoming a major form of crime. "One" here refers to the individual Internet user —an independent computer terminal in cyberspace. At the Web 1.0 stage, the major users of the Internet were commercial bodies and portals; individuals were recipients of online information rather than real participants in online activities. Online interests focused on computer systems of varying size. During this period, cybercrime meant an attack mounted by an individual on the computer systems of large organizations. In form, it was a challenge posed by the weaker party (the individual) to the stronger (large organizations). At the Web 2.0 stage, the Internet has become the basic platform of human life and ordinary net users are becoming real participants in online activities. Cybercrime too has switched the target of its online attacks and attacks on the general public have become a major option. (2) The relationship between perpetrator and victim. A real life one-to-one injury has changed into a one-to-many injury in cyberspace. The result is that it is not possible to be certain about the injured party. For example, after completing integrated vulnerability scanning, a softeare can be employed to attack tens of thousands of networked computers. At the same time, as the Internet overcomes restrictions of time and space, an attack may produce a ripple effect through the whole system. The 5-19 Internet disconnection incident is a case in point. On May 19, 2009, a DNS (domain name system) server was the subject of a botnet traffic attack, leading to an error in the DNS of media transmission software. As a result, the telecommunication network in nine provinces and cities was paralyzed.

II. Concrete Examples of Cyberspace Variants in Traditional Crimes and Associated Reflections

From the judicial perspective, a crime committed in actual space can readily be handled by existing laws, but when the same crime is committed in cyberspace it is often hard to assign criminal responsibility. In what ways do differences in cybercrime manifest themselves? Unless we can find way of dealing with this question, traditional criminal law will be fighting "imaginary enemies."

1. Cyberspace variants of constituents of traditional crimes

The rapid diffusion of the Internet has fundamentally changed the "raw material" and "elements" that make up a crime. This includes changes to the following constituent elements of the crime: the injured party, the offence, the motive and the consequences.

(1) The changing concept of the injured party in cyberspace

As far as the criminal act is concerned, cybercrimes may be no different from traditional crimes. However, the difference in the injured party may present barriers to the application of traditional criminal law.

a. The emergence of virtual property in cyberspace

The emergence of virtual property was inevitable as the Internet shifted from being an information medium to being a life platform. Typical virtual property includes electronic game items, QQ numbers, etc. Its physical significance is merely that of digital symbols or information codes; they can be controlled by humans but cannot exist offline. One of the controversies about virtual property is whether it enjoys the protection as the "other property" stipulated by Article 92 of China's Criminal Law.[1] The theft of a QQ number illustrates this point. The suspect, a Mr Zeng, a former employee of Tencent, stole Tencent's QQ "lucky numbers" and resold them to other QQ users, reaping a profit of more than 70,000 yuan. During the trial, plaintiff and defendant engaged in heated debate. The former argued that the QQ numbers were an informational product and possessed the characteristics of physical property, so that Zeng had committed theft. The latter argued that the QQ numbers were only a kind of code service and there was no basis in law for determining their nature. Therefore, Zeng was innocent. The court trying this case bypassed the issue of whether QQ numbers constituted virtual property and ended up regarding them as communication codes and defining the case as one of injury to freedom of communication. In this way, they skillfully sidestepped a determination on the nature of virtual property.

By its nature, virtual property is still a kind of property, it is just that the online factor has changed the form in which it exists. How, then, does such a change affect people's understanding of the nature of property? One might say that the division of property into

1 See the judgment delivered by the People's Court of Nanshan District of Shenzhen, Guangdong Province, no. 56 of the First Trial, January 13, 2006, the People's Court of Nanshan District, Shenzhen, Guangdong Province.

tangible and intangible and subsequently into actual and virtual shows that the diversity of forms of property is itself a developmental tendency.[2] As the quantity and forms of virtual property increase, we should confirm virtual property as being a form of property under criminal law and entitled to the law's protection. This would serve the interests of the injured party.

b. Thoughts on botnets and renting/selling from the perspective of criminal law

"Botnets" are connected with "Trojan horse" programs. Computers attacked by the latter are often called zombie machines. A whole computer network composed of zombie machines controlled by the same Trojan horse client is called a "botnet." This has already become a favorite tactic of cyber criminals. The disconnection of network services on May 19 was the result of hackers' attack on the computer network via a rented botnet. Existing criminal law could be employed to crack down on the illegal control of other computers by means of a Trojan horse. However, it is powerless to stop the renting, reselling and transfer of botnets.

In essence, a botnet represents the control of computer terminals by a Trojan horse programs. It involves the illegal use of web resources in a non-exclusive manner. In other words, it affects computer users' right of use rather than the ownership of the computers. This is like driving a stolen car in real life: the perpetrator does not intend to possess someone else's car illegally, but does intend to drive it illegally. Therefore, both a botnet and driving a stolen vehicle are essentially a kind of "theft of use". For this reason, the law bases its assessment of botnets not on the renting and reselling of botnets themselves but on the underlying relationship in criminal law between theft and use. There are many types of "theft of use" in cyberspace, including illegal use of other people's broadband, illegal use of computing facilities, etc. Hence, although the use of botnets is common and extremely damaging, it does not constitute a category of behavior of the kind the law concerns itself with, being at best some kind of "species" of behavior; it is the more general "genus" of behavior—theft of use in cyberspace—that fits the law's categorization of crimes. As a result, a solutions to the problems occasioned by cyberspace variations in traditional crimes may depend on the improvement of traditional criminal law.

(2) Cyber variants of crime

Cyberspace serves as a new platform for crime but most cybercrimes are just new versions of traditional crimes. However, the fact that the platform has changed does influence how the crime is assessed.

a. Traditional offences that utilize weaknesses in computer programs

Traditional criminal theory tends to hold that a machine cannot be the object of fraud as it does not have an independent will and therefore cannot make mistaken judgments on the basis of mistaken understandings that lead to voluntary action. Therefore, utilizing the weak points of computer programs to acquire property is defined not as fraud (since the machine does not have free will) but as theft. However, committing a crime in this way is the same as

2 Gunther Artz *et al*., *Strafrecht BT*, p. 315.

committing fraud involving machines in a traditional crime. For example, a suspect, Mr Yi, used defects in the Netease online sales system and delays in updating its web page to alter the original amount paid, so that he paid one cent each for 340,000 cards worth 5.07 million yuan. In this case the Procuratorate argued that Yi's act constituted theft, but the court ended up defining it as a case of fraud, for two reasons. The first was that his purchase of virtual cards via the Internet was a normal business transaction involving the assent of both parties and was a function of their joint intention. It was thus not a theft, which is carried out by the will of one party alone. The second reason was that the entire transaction was conducted online. On the surface, Yi was interacting with a computer system. However, the Netease digital sales system operated according to the programs designed by its computer programmers, which embodied the original intentions of Netease. Thus it was Yi's "switch" at the payment stage that gave Netease the mistaken impression that full payment had been made, on which basis it had voluntarily sold him the cards. Yi was tried for fraud.[3] In this case, the court attempted to use the idea that "the program embodied the original intentions of Netease" to argue that the Netease program had an independent intention by virtue of the transfer of "intention." However, there is inadequate evidence for the idea that a computer program effectively embodies or can be equated with the initial intention of its designers. As a matter of fact, even the highest judicial authorities have no definite opinion on this point. In 2008, in its "Official Reply on the Categorization of Picking Up a Credit Card and Using It to Obtain Money from an ATM," the Supreme People's Procuratorate acknowledged that an ATM could be the target of fraud. However, in its 2003 "Reply on the Application of the Law in Relation to Illegal Production, Sale and Use of IC Cards," it did not acknowledge that IC telephones could be the targets of fraud. Objectively, as these judicial debates increase and with them the dilemmas of the judiciary, we urgently need follow-up work on criminal law theory and amendment of criminal law norms.

b. Assessing abuses of software technical protection measures

The Microsoft "Black Screen" event is a prime example of the abuse of software technical protection measures. WGA (Windows Genuine Advantage) is an anti-piracy system created by Microsoft in 2008 that carries out online validation of the licensing of Microsoft Windows XP, etc. Users with pirated copies saw only a black desktop screen on opening their computers. However, this elicited widespread public criticism. In fact, there are numerous such cases. The 1995 word processing software CCED 5.0 and the 1997 anti-virus software KVL 300++ both contained harmful programs inserted by their copyright holders that would lock the computer hard drive or wipe out data once the use of pirated copies was detected. It could be said that software developers' abuse of software technical protection measures has become commonplace.

The existing criminal law has no regulation dealing directly with this issue. As these abuses happen in cyberspace, their negative impact has received scant attention and evaluation.

3 See the judgment delivered by the court of Haidian District of Beijing, No. 87 of the First Trial, April 20, 2007, the People's Court of Haidian District of Beijing.

But if similar abuses happened in actual space, they would undoubtedly be attended to and evaluated by criminal law. For example, if you installed electric fences around your own vegetable garden so nobody could steal the vegetables and a would-be thief received a fatal electric shock, your purpose might be legal but your tactics would pose an actual or potential threat to public security, so you might be punished by criminal law. At present, some software developers have employed punitive technical protection measures in the name of copyright protection in a way that already threatens "public security" in cyberspace. If the damage caused by this kind of behavior reaches a certain level, we should consider invoking criminal law and the possibility of assessment. As to what we call the charge, those in traditional criminal law should do.

(3) Cyber variations in the consequences of crime

Among cyber variations in the consequences of crime is the fact that the line between direct and indirect consequences becomes blurred. The former generally refers to the harm directly caused by the harmful act whereas the latter refers to the harm indirectly caused by the harmful act. The distinction between the two is whether there exists an independent phenomenon that acts as a medium connecting the act and its consequences.[4] However, the line between them has become increasingly blurred in cyberspace, where the connections between information systems are much closer than those between things in the real world. The Internet is a whole made up of innumerable interconnected information systems and an attack on any link in the chain could paralyze the whole system, as in the 5.19 Incident. In the real world, for example, if A beats B to death and B happens to be the manager of a key project in a factory, the death of B may cause this project to miscarry, leading to huge losses for the factory. Whether or not A knows B's position, B's death is the direct consequence of A's criminal act but the losses of the project are not. However, in cyberspace, if a natural person, A, attacks server B and paralyzes it, at the same time, since server B cannot provide normal service, none of the websites under it can be visited. This situation should be regarded as the direct consequence of A's attack.

Cyber variations in the consequences of crimes is also seen in the fact that it is difficult to determine consequences accurately. The limitless expanse of the Internet in terms of information transmission enables information to multiply and be transmitted rapidly. This means that the consequences of cybercrime extend endlessly, directly leading to the difficulty in determining what they are. The spread of computer viruses illustrates this point. Such viruses may lie dormant in a computer's information system in a computer, ready to break out at any time. However, they are virtually undetectable before they break out, and it is very difficult to calculate accurately either the number of computers infected or the damage caused when they do break out, especially when their effects may be lasting. For example, the well-known virus CIH emerged on a large scale every April 26 from 1999 to 2004 and still breaks out sporadically today, albeit on a smaller scale. Consequences

4 Gao Mingxuan and Ma Kechang, eds., *Criminology*, p. 80.

of this kind, lasting several years, mean that it is clearly impossible to make an accurate estimate of the consequences at the time when the crime is committed or shortly thereafter. As a result, we need to explore new and more practicable feasible standards for quantifying the consequences of cybercrime.

(4) Cyber variations in criminal intent

Among cyber variations of traditional crime, the one that has caused the greatest trouble and confusion for judicial practice is the question of variants of criminal intent in the form of the profit motive. An example is the "Coral case." The defendant, a Mr Chen, developed a Coral software enhancement that optimized the functions of Tencent's QQ software but did not change any of its program code. The enhancement could not run independently but required QQ software. Chen packaged the enhancement together with QQ software on his own website for downloading but added ads and commercial plug-ins for which he received payment. This was the key circumstance in the court's determination of whether Chen had infringed Tencent's copyright for motives of profit; the issue lay at the heart of the debate between the two sides to the case over whether Chen's act constituted a violation of Tencent's copyright. In similar fashion, for-profit online bundling of advertisements and plug-ins with third party software has become a grey industry, so the ruling in this case will to a certain extent also decide the fate of third-party software.

Does "adding paid advertisements and commercial plug-ins" fall under the profit motive? The vast majority of netizens stood on the side of Chen, the defendant, but the court held that Chen acted out of the profit motive. We support the point of view of the judicial organs, which can be explained in terms of a similar case in the real world. For example, following international practice, the telephone book or Yellow Pages produced by China Telecom is distributed to the public free of charge even though it has high production costs. The costs are recouped through advertising charges. In practice, many illegal advertising companies replace the Yellow Pages ads with ads for which they have been paid and print and distribute Yellow Pages to the public themselves. This practice and Chen's actions in the Coral software case are in essence cut from the same cloth. It is hard to deny that these illegal advertising companies are not actuated by the profit motive. In independently posting the enhanced version of Coral software on his website for downloading, Chen was not violating anyone's copyright. By bundling the enhancement with legal software, Chen was actually making use of the platform of the legal software, so our understanding of the "profit motive" cannot divorced from an examination of the legal software. However, it should be noted that although there are cyber variations in the "profit motive," the issue can legitimately be resolved through judicial interpretation within the framework of the existing criminal legal system.

2. Cyber variations in negative social impacts of traditional crimes and some reflections

Cyber variations in the negative social impact of crime can be characterized as reproduction, focusing and diffusion.

(1) Online reproduction constituting an offence harmful to society

The Internet may contribute to reproduction of the element in crimes harmful to society both horizontally and vertically. In terms of horizontal reproduction, we can take the example of the online transmission of copies that infringe copyright. In traditional space, copyright is attached to a particular physical vehicle that incorporates a cost. As a result, no matter how serious the infringement of intellectual property is, it has objective limits. The digital form of intellectual property throws off the limits of its physical vehicles; the amount of storage space it occupies may be infinitesimal but there are no physical limits to its transmission. In terms of vertical reproduction , cyberspace contributes to a dramatic increase in the number of such crimes. With the advent of cyberspace, the previous single platform for commission of an offence, "cyberspace" has been added to "real space," providing two platforms. A single offence can be committed entirely in cyberspace or can span the two platforms of cyberspace and real society. The coexistence of the two not only gives criminals more resources but also lowers some traditional thresholds to the commission of crime, whence the steep climb in criminal activity.

(2) Focus as an offence harmful to society

The focusing effect of cyberspace objectively influences our understanding of the negative impact of crime on our society. Let us analyze the example of bad links provided by search engines. Originally, such links are a classic one-sided joint crime. In that they contribute to offences and the transmission and diffusion of harmful information, they should be regarded as auxiliaries in joint crime as their injurious nature is less than that of the principal offender. But links do play a genuine role in spreading information. Compared to the linked information, search engines take the initiative and perform the guiding role. At the same time, a search engine may connect to a sea of information and web pages and this exaggerated form of a one-to-many relationship means that links that were originally regarded as subordinate and auxiliary acquire a harmful role through the aggregation, focusing and strengthening of information. Let's take the spread of pornographic material as an example. Viewed in isolation, links need only bear responsibility for the specific amount of pornography information retrieved from the Internet on each occasion. In most cases, this is quite limited and constitutes an offence rather than a crime. It follows that from the perspective of the traditional theory of accessories in joint crime, the link itself does not constitute a crime. But if we look at the situation as a whole, all of the pornographic information scattered over the vast expanses of cyberspace can be found and aggregated by means of these links, so that the Internet links are in themselves an act of communication. In such circumstances, the individual who sets up the links should be responsible for all the pornographic information spread by those links. Like a magnet, search engines have the function of "attracting" and aggregating information. The aggregating function is that of the link, with the "attracting" function being dependent on the strength of link. As a result, the act of Internet linking should be given independent status in legal assessment, doing away with its status as a joint crime so that the perpetrators can be dealt with as principal offenders.

The focusing of the Internet can also have another effect: that of rapidly focusing the originally dispersed attention of the public on a specific act or event. Thus a crime's evil influence or the sympathy factor involved are rapidly magnified, thus either magnifying the harm caused (in the case of evil influence) or diminishing it (in the case of a sympathy factor). Take the "HIV Slut" Incident as an example. Yan Deli, the victim of an Internet smear campaign conducted by her ex-boyfriend Yang Yongmeng, was falsely rebuked for working as a prostitute and spreading AIDS intentionally. Yang was finally convicted of aggravated defamation. The focusing effect of the Internet had an enormous and shocking effect on the victims and on social order and eventually led to the case being elevated from "a case accepted at complaint only" to one of "serious harm to public order and national interests." It should be noted that any piece of information posted on the Internet may be known, scrutinized, communicated and evaluated by innumerable recipients so that its influence grows exponentially. What is awkward is that if two similar criminal acts occur at the same time and one attracts the focusing effect of the Internet while the other does not, we will evaluate them very differently. Therefore, we should be concerned with the way the Internet's focusing function increases and diminishes the degree of harm done to society by the criminal act. There are more and more cases in which the Internet "gives a hand," and the phenomenon of fabricated Internet concern is having a serious impact on the evaluative model and criminal law theory. This affects judicial fairness and independence.

(3) The online diffusion of the negative social impact of a crime

The Internet's diffusion effect on the negative social impact of crimes is exemplified in online hacker technical training. The rapid development and spread of hacker training schools has led not only to the dissemination of hacking techniques but more importantly, to a rapid increase in cybercrime. Hacker training schools have also become systematized into a link in the hacker industry. (Motivated by its own interests, this industry link has developed from the writing of computer programs to disseminating and selling them and laundering the money. The buying and selling of virus and attack programs already constitutes a complete branch of the industry). This demonstrates the way the Internet's new support role has shifted from "providing tools" to "providing techniques." In essence, hacker training provides technical assistance to the hackers' subsequent criminal acts; by its nature, this falls into the category of being an accessory to the principal offender. However, the harm such assistance does to society may be many times greater than that occasioned by the acts of the principal offender. Looked at in isolation, hacker training schools should be responsible only for the hackers' subsequent criminal acts and the harm caused should not exceed that caused by the hackers' subsequent criminal acts. However, it is precisely the hacker training schools that catalyze all the subsequent criminal acts performed by the principal offender. Each of these acts derives from the hacker technical training, so such training should, of course, be responsible for all the acts of the principal offender. It is this that is the true face of the harm done to society by hacker technical training. The "one-on-many" model of crime is having a profound effect

on assessment of the negative social impact occasioned by the acts of online accessories. This situation, in which the acts of accessories have caused greater damage than those of the principal offenders, would have been hard for traditional criminal law to have imagined.

3. Cyber variations in the form taken by traditional crimes and some reflections

The Internet has an influence on the form of crimes that is three-dimensional rather than flat. In joint offences, technological support is assuming a more and more prominent role in crime as a whole. Its actual function and its share in the social harm caused are much greater than was the case with traditional crime. This has led to a switch in the roles of the accessory to and executor of a crime and to a total change in criminal law's action plan and evaluation system. For example, at the end of 2007, the defendant, Li Kang, discovered in the course of helping an associate forge documents that he would be able to make a lot of money by verification data stored in computer systems. He and one Li Hang therefore planned to drop Li Kang's previous associates; Li Hang was to liaise directly with people who wanted computer data, while Li Kang would be responsible for hacking into the computer system to add the information. In the following year and a half, Li Hang used tool softwares and "Trojan horse" programs, etc. on a number of occasions to hack into several Shaanxi databases, where he changed and added 1289 pieces of data on job titles and qualifications. They made a corrupt profit of 1.3 million yuan.

The web element's penetration into this kind of forgery led to two cyber variations. (1) A variation in the form of the termination of a crime. In the past, the criminal act ceased with the production of the forged document. Now, however, as the information needed to verify a document is stored in an online databank, the forgers need to take the extra step of hacking into the databank to add the false information; only thus can they guarantee the normal use of the document. For this reason, the subsequent act of hacking into the computer system has inserted itself into the forgery process and become a component of the crime. Objectively, this lengthens the physical process of the crime and makes its completion in physical space into preparation for a crime in virtual space. (2) Variation in the form of joint offences. In this case, Li Kang was originally helping the forgers add additional data stored in the computer system. This act, by its nature, was that of an accessory to the principal offender. However, as Li Kang found that hacking into the computer system and tampering with the data became a lucrative proposition, he went out on his own, so that the previous principal had to turn around and ask Li Kang for help. The reason was simple: without Li Kang's "help," a plain forged document was completely "non-competitive" in the market. This implies that the prominence of "cyber forgery" of documents has led to the swapping of roles between the accessory to and the executor of a crime, with auxiliary acts rising to the status of principal acts and principal acts diminishing into auxiliary acts.

III. Cyber Variations in Traditional Crimes and Responses under Chinese Criminal Law

In the face of the mounting tide of cybercrime and the public call for the criminalization of

harmful online acts, we need to think carefully about how necessary criminalization is and what should be its limits.

1. The theory of cyber variants of traditional crimes and basic legislative response

One of the prerequisites for criminalizing harmful online acts is that the traditional criminal law fails to evaluate or judge such cases. Though the trend toward cyber variants of traditional crime is extremely clear, an extended interpretation of current criminal law can resolve the great majority of cases. As some scholars have suggested, it is not hard to apply current criminal law interpretations to cybercrimes. Ordinary criminal laws that served to deal with horse-stealing several centuries ago still apply in the age of automobiles and aircraft and will apply in the age of information technology. A case in point is that though the US Congress passed a Counterfeit Access Device and Computer Fraud and Abuse Act in 1984, there have been few prosecutions under it, mainly because much computer crime can be prosecuted under a different title. There is thus no need to keep introducing new legislation for cybercrimes. Rather, existing legislation can be amended in those few articles that present difficulties of interpretation.[5] In most cases, the computer has not initiated a completely new type of crime. Rather, it has altered the ways in which old crimes are committed.[6] Thus many cybercrimes are merely the re-emergence in cyberspace of traditional crimes; the only difference is that technological factors have intervened. The problem can be dealt with by updating criminal law theory and the rules of interpretation and using legislation designed for traditional crime to cover new crimes. Introducing new legislation to tackle cybercrimes is only necessary in those few cases when cybercrimes do infringe provisions on a completely new set of legal rights or interests.

2. The extended judicial interpretation approach: interpretation of the treatment of joint offenders as principal offenders

In most cases of cyber variations in traditional crimes, extended judicial interpretation is quite capable of handling the issue. A specific interpretative approach is interpretation of `joint offenders as principal offenders.

(1) The establishment of a judicial model for interpreting treatment of joint offenders as principal offenders

This model offers an effective means of ascertaining the criminal liability of someone who provides technical help for a criminal act in cyberspace and has been gained acceptance in practice. For example, in 2010, the Supreme People's Court and the Supreme People's Procuratorate comprehensively confirmed this model in "Interpretation of Some Issues Concerning the Application of Criminal Law to Handle the Use of the Internet, Mobile Telecommunication Terminals and Information Services to Produce, Reproduce, Publish, Sell and Disseminate Pornographic Information" (2) (abbreviated below as "Pornographic Information Interpretation" [2]). For example, the fourth article determines that anyone who sets up a for-profit website or is directly responsible for its management

5 Liao Youlu, *Some Criminal Issues in Cybercrime*.

6 G. Jack Bologna and Robert J. Lindquist, *Fraud Auditing and Forensic Accounting*, p. 221.

and is aware that that website or web page is being used by others to produce, reproduce, publish, sell and disseminate pornographic information with their permission or because of their failure to intervene, should, in serious cases, be charged with disseminating pornography and sentenced accordingly. This new interpretation of the four types of technical support involved no longer defines them as the acts of an accessory, but rather, assesses and punishes them as the acts of an executor directly engaged in disseminating pornography or disseminating pornography for profit. It no longer takes into account whether the transmission of pornography for which they provided support constituted a crime, nor does it provide a fixed assessment of the crime of disseminating pornography or disseminating pornography for profit. This reduces complications: the step of identifying and evaluating specific acts of disseminating pornography can more effectively assess and punish the technical support services on the Internet that represent a greater threat to society. Clearly, this represents the establishment of the principle of making joint offenders into principal offenders.

(2) The judicial dilemma of the limits to expanded judicial interpretation

The strategy of making joint offenders principal offenders has its limitations and may give rise to certain judicial dilemmas. We analyze this issue by citing the fourth article of "Pornographic Information Interpretation (2). Although this article stipulates that the supporting acts of people who set up and manage websites should be assessed as acts of execution, it raises the level of the criteria for an offence by requiring a certain "frequency" or "consequence" of the act. Specifically, supporting acts cannot be regarded as acts of execution unless their frequency is five times that prescribed for acts of execution or twice that prescribed for acts of execution in the case of two forms of support, or unless there were grave consequences. However, another question arises: what if the supporting acts of an accessory fail to meet the criteria for a crime? For instance, if a web manager lets someone post pornographic information on the Internet but it is insufficient to meet the criteria for a crime, no crime has been established. However, if the material posted does meet the criteria for a crime, the web manager should be deemed a joint offender and consequently his acts constitute a crime. Therefore, the question of whether the acts of the joint offender constitute a crime is dependent upon the question of whether the acts of the principal offender constitute a crime. If they do, the web manager could be prosecuted as an accessory; if they do not, no crime has been established in the case of the web manager. The reason for such a judicial dilemma is that the interpretation of online technical support characterizes it in two different ways: as a supporting act in a joint offence and as the act of execution in a sole offence. The way the dual nature of a single act is interpreted must necessarily lead to two different judgments on a single act. Consequently, there will be a conflict and contradictions between the definitions of what is a crime in particular cases. Thus extended interpretation does have its limitations. In the face of the trend for wholesale change in traditional crimes, it is imperative that China's judiciary explore a set of solutions at the level of criminal legislation.

3. Judicial responses to cyber variations in traditional crimes: makes acts of preparation

into executive acts and joint offenders into principal offenders

In the face of cyber variations in traditional crimes, criminal legislation has witnessed two completely new approaches.

(1) Response to the multiplication of the harmful effect of negative online behavior: the tendency to raise preparatory acts to the status of executive ones and make them independent.

Let's elaborate on this point by using hacking into a computer information system as an example. In terms of jurisprudence, illegally hacking into a computer information system should be regarded as a type of preparatory act to stealing secrets relating to national affairs, national defense secrets and cutting edge science and technology secrets. Considering the gravity of such preparatory acts, some criminal law theorists argue that their initiation or completion would inevitably produce a negative impact that would be hard to foresee, assess or recover from. On the other hand, even if such acts were completed, they would not necessarily produce the actual consequences we identify, at least not at once, nor will such acts necessarily ultimately be detected or verified. In view of their gravity and special characteristics, China's Criminal Law 285 stipulates that these substantially preparatory acts be elevated to the level of executive acts, to strike hard against this type of crime. In subsequent criminal legislation related to cybercrime, this legislative option will become common.

(2) Response where the negative impact from supporting acts in cyberspace would be too great: making the joint offender the principal offender

It has to be said that in traditional crimes it would not have been possible for the harm caused by an accessory to be greater than that caused by the principal offender. However, this is common in cyberspace. Unlike traditional joint offences, the supporting acts occurring in cyberspace have been replacing acts by the principal offender as the core of joint offences. Therefore, criminalizing supporting acts in cyberspace that may have a serious impact on our society, treating joint offenders as principal offenders and making supporting acts independent crimes offer the best response to the actual challenge posed by joint offences on the Internet. The legislative model of making joint offenders into principal offenders will become a commonly used legislative option for cybercrime and more and more supporting acts online are likely to be treated as independent crimes. If we take a look at the newly added articles relating to cybercrime in the Amendment to Criminal Law (7), we find that it in fact follows the approach of treating joint offenders as principal offenders.

IV. Conclusion

Cyberspace provides new space for traditional types of crime. Cyber variants of traditional crimes have severely affected and eroded the effectiveness of traditional theories of criminal justice and have weakened and hollowed out traditional criminal legislation in a way that cannot be retrieved. The Internet's impact on traditional criminal legislation is increasing; it is no longer limited to general regulations and articles but has to erode its fundamental

theoretical framework.[7]

Born in agricultural society and growing up in industrial society, our systems of traditional criminal law theory and legislation are unable to keep up with the information society. In the face of the constant development of network technologies and their increasing penetration of traditional crime, traditional criminal law theory and legislation risk lagging behind the reality. Therefore, we should face up to the challenges posed by cyber variants of traditional crimes and take a holistic approach to the relationship between the Internet and criminal law from a higher and broader perspective, to encourage an epochal transition in the traditional legal system.

Notes on Contributor

Yu Zhigang, Professor of the College of Criminal Justice at China University of Political Science and Law (CUPL). Main interest: science of criminal law. Major works: *The Expanded Interpretation of General Principles of Criminal Law* (刑法总则的扩张解释, Beijing: China Legal Publishing House, 2009), *Values in Crime* (论犯罪的价值, Beijing: Peking University Press, 2007), *The Principles of Criminal Law in Cyberspace* (网络刑法原理, Taiwan: Yuanzhao Publishing Company, 2007), *The Theory of Criminal Law in Virtual Space* (虚拟空间中的刑法理论, Beijing: China Fangzheng Publishing House, 2003) and *Research on Systems of Eliminating Punishment* (刊罚消灭制度研究 Beijng: Law Press, 2003). E-mail: yuzhigang9774@sina.com. Address: Graduate School of China University of Political Science and Law, 100088.

References

Artz, Gunther *et al*. *Strafrecht BT.* Bielefeld: Ernst und Gieseking, 2009.

Bologna, G. Jack and Robert J. Lindquist. *Fraud Auditing and Forensic Accounting*. Trans. Zhang Yu. Beijing: China Auditing Press, 1999.

Gao, Mingxuan and Ma Kechang, eds. *Criminology* (刑法学) Beijing: Peking University Press and Higher Education Press, 2003.

Liao, Youlu. *Some Criminal Issues in Cybercrime* (计算机犯罪的刑法问题). *Journal of Central Police University* (“中央”警察大学学报 [台南]), 1997, vol. 31.

Smith, Russell G. *et al*. *Cyber Criminals on Trial*. Cambridge: Cambridge University Press, 2004.

—*Translated by* Liu Hui *from*
Zhongguo Shehue Kexue (中国社会科学), *2010*, *no. 3*
Revised by Sally Borthwick

7 Controversies in this aspect are also reflected in the name and implications of the wording of criminal legislation. In legislative nomenclature, “cybercrime” and “cyber crime” differ not only because one is a word and the other a phrase, but also because to a certain extent they actually determine the implications and scope of criminal legislation. See Russell G. Smith *et al*, *Cyber Criminals on Trial*, p. 5.