Research on Criminal Liability of Cybercrime Related to Attack Cloud Storage Platform

Lv ZHAO
Zhejiang Police College, Hangzhou, Zhejiang, China
2539592434@qq.com

Keywords: Cloud Crime, Criminal Liability, SPSS.

Abstract. Attacking cloud platform crime is a kind of crime which is extremely harmful in the web3.0 era. It has the characteristics of strong combination ability, miscellaneous legal infringement category, low crime cost and difficult combat. In order to better criminalize this kind of crime, in addition to the traditional theoretical research of academic circles, it is necessary to study the trinity of practical research, data support and theoretical research. This article starts with the criminal model of attacking the cloud platform, sorts out 300 cases of the referee paper network, and the 42nd "Statistical Report on the Development of China's Internet Network" and other related data, and investigates the relevant substantive departments, and strives to clarify the crime of attacking the cloud platform. "Combining with other cybercrime, analyzing the existing loopholes in criminal liability system, providing a reliable basis for scientifically identifying crimes and managing the network society."

Introduction

Since the forty years of reform and opening-up, our core technology such as cloud computing and big data is close to the internationally advanced standard, big data platform, industrial cloud and industrial big data technology is built more and more quickly, aiming to forge "China Science and Technology cloud". At the same time, the crime in the information age makes a profound difference as well, its crime mode is transferring from computer crime to cybercrime, changing into cloud crime meanwhile, the mode of conviction and measurement of penalty of traditional cybercrime is challenged seriously. In view of this, this paper will use SPSS17.0 software to analyze data, basing on the analytical conclusion, to provide data support for theoretical research and discuss the related dispute.

The Analysis of the Crime Pattern

It is generally acknowledged that cloud platform uses cloud computing and cloud storage as the platform, by clustered application, hierarchical storage, DFS (Distributed File System) and other storage device and software and hardware facilities, providing data storage and transaction access to outsiders together. At the same time, countless users will willingly transfer some or all the ownership of the data to management organization in order to gain corresponding right. However, when using SPSS graphics software to analyze the data in the 42th Statistical report on the development of the Internet in China, we get that 3-D bar chart (Figure 1) and discover that cases in which masses of personal information are given out and account and password are stolen have the tendency of increasing.

Tracing the evolution of cybercrime, we can find that there exist two intergeneration leaps in it. In Pre-internet age, computer system is considered as crime target and require protection from criminal law by such typical cases as encountering virus or password being stolen. As the web1.0 era is coming, Internet has become the criminal tool, embodying in the prevailing of Internet fraud. In current Internet phase, Internet has become the crime space gradually. At the same time, the arrival of cloud era provides the possibility of salutation for cybercrime which is considered as “target of crime” and “criminal tool”, so as to promote the fusing of three types of crime. [1]
For current types of cyber crime, after searching three hundred cyber crime cases from 2013 Jan. to 2018 Dec. and using SPSS Graphics software, we get a crime pattern (figure 2), that is the combination of "attacking cloud storage to stole information” and “other network crime”.

Figure 1. The Chart of Comparison of Internet Security Incident between 2017 and 2018.

Figure 2. The Criminal Process of Attacking Cloud Storage Platform and Its Related Cyber Crime.

Attacking Cloud Storage Platform and Stealing Information

Netizens release the absolute ownership of data by sharing API. Different kinds of information are based on Internet, keeping away from desktop [2] government, enterprise and individual can help themselves according to their own demand. Suspects use natural shortage of cloud computing[3] combine hacker technique and then attack base station and steal password, format contract and other ways to “steal” information openly with the advantage of duty. For this, I would analyze this process from the angle of “alternation of new and old criminal skills” and “aberrance of aggressive behavior”.

The Alternation of New and Old Criminal Skills. Seeing from criminal skills, when taking the first half of 2018 for example, we’ll find that the type of cyber security incident still focus on traditional cybercrime. However, when seeing from absolute numbers, tampering the number of webpage, website which is implanted back doors, fake website and other cyber crime show the tendency to mutate and surge. By using SPSS graphics software, we get figure 3 and discover that crime of network virus and computer virus attack has decreased sharply in web1.0 era when compared to crime of attacking website in web2.0 era. In other words, method of attacking cloud storage platform is at the stage of “transition from old to new” and present the characteristic of self-evolution. Now, whether the way of affirming and explaining traditional cybercrime is possible to apply to cloud crime is worth lawmaker’s thinking.
From another perspective, the transition from old to new criminal skills will not only influence pattern and thought of making law, but also overturn the way of thinking and studying technology which user and operator use to deal with computer information and network interconnection, then we will achieve inclusive development of computer technology and network technique in the process of differentiate them.

**Figure 3. Variation of Aggressive Behavior.**

**Variation of Aggressive Behavior.** Ubiquitous-cloud of various software and applications make the process of storing, flowing, keeping and using personal information recorded in the cloud. For cloud not only exist in network era but also in real life, it becomes the bond of dual society, and enable it with Synchronization, real-time, stability and other characteristic and turns into a kind of normal growth and future in the information era. Whereas, in the course of Ubiquitous-cloud, different kinds of invasive behavior exist extensively which can be divided into “transactional” “spying” and “leaking”. [4]

With the support of new technology platform which does away with desktop, the proportion and rate of invasive behavior increase sharply, not only limited to the invading pattern which can be induced between border and point-to-point. However, in the background of Ubiquitous-cloud, the mode of encroach legal rights present the characteristic of concentrated outbreak and extensive influence. Taking the first half of 2018 for example, information of Saks and Lord & Taylor company which is attacked by Hacker group and given away is up to 5 million, and Pump Up company’s not encrypting back-end servers causes 6 million pieces of information to be leaked. At the same time, Sacramento Bee company is attacked an anonymous attacker, leading to 19.5 million pieces of personal information given away.

**The Mutation of Criminal Case after Attacking**

After attacking cloud storage platform, it achieves the aim of catalyzing traditional crime and create new type of crime by transferring all kinds of data of computer information system through instant communication tools and other transmission methods.

The network crime in our country can be divided into two kinds approximately, namely traditional crime networking and new type crime diversifying. The former one presents the features of illegal property alienation which reflects in crime field, crime tools and crime target networking. Nevertheless, the latter one presents the dilemma of our country’s traditional response pattern of ”two tracks, three points and four lines” whose crackdown and means are limited when attacking new type crime. In terms of the former one, crime field, tools and objects shows the trail of mutual integration and running parallel in web3.0 era. With telecom fraud as example, after a long time’s self-evolvement, suspects use “Four-in-one” method which contains phone, Internet, telephone and TV, adopting the Internet information technology of mobile Internet, [5] from the “large sum of money
for child”, ”guess who I am” and other ways of fraud which is blanket at the beginning. And then it develops into information organizing and analyzing, verbal trick compiling, victim filtering out, fraud carrying out, “cash for others” quickly and other industrial fraud way. According to the report Research on the Tendency of Internet Fraud in 2018 [6] which is released by Hunting net Platform, in 2018 all year round, Hunting net Platform received valid report 21703 cases in total, and the total amount hustled is up to 3.9 billion, per capita losses is 24476 yuan, the highest level since five years ago, increase about 69.8 percent compared to the same stage in 2017. However, in order to achieve the innovation of crime skills, the premise is the accuracy of criminal information and intelligence.

During the process of organizing three hundred Internet crime cases on judging paperwork net, we find that the way of attaining criminal information and intelligence changes from passive reception to active obtaining, its way and method of acquiring also have a big change. From 2013 to 2014, suspects mainly attain citizen’s personal information by installing locator or inquiring Public Security network, the pathway to get information presents the trait of unicity and finiteness. Since year 2015, the number of cases of invading citizen’s personal information increases sharply, as figure 4 shows. At the same time, the way of gaining citizen’s personal information presents the strengthening of dependency of Internet and universality of range of gathering, as figure 5 shows.

![Figure 4. Figure of Number of Crime of Stealing Citizen’s Personal Information from 2013 to 2018.](image)

![Figure 5. Schematic Form of Way to Access to Citizen’s Personal Information.](image)

From the above, crime patterns of attacking cloud storage platform and other cybercrime are mainly composed of two parts, namely acquiring citizen’s personal information by attacking cloud storage platform and carrying out other cybercrime which are represented by telecom. As a chain of crime, every part is an independent unit, presenting the characteristic of relevance which coexists with independence. Now, there are rules which outlines the legal system with No.38,39,40 of constitution at the lead, No 285,286,287 of penal law and The decision of maintaining network security which NPC (National People’s Congress) made as main line, Network Security Law, Passport Act, Statistic Act.
and other civil law and social law as addition, six judicial explanation as focus. However, in the designing of guilty, it demonstrates the trait of theory of accomplice vague, the standard of incriminating inappropriate, the protection of Criminal Law corresponding with the harm to society, which result in the difficulty of obtaining evidence in the stage of preliminary hearing and investigating, trouble of applying to law in prosecution and trial stage.

**Regulatory Hurdles**

The cybercrime of attacking cloud platform presents the mode of chain, if we think about the component units of crime of chain further, we can divide it into group type crime, cyber gangs and “lone wolf” crime three types. In practices, the mode of group type crime presents the characteristic of big harm, high degree of integration, difficulty of imputation, being the main target which practice authority attack. Therefore, this article will mainly talk about the dilemma of preventing this kind of mode.

The Internet criminal groups of attacking cloud platform can be divided into network attacker, information provider, other crime executor, people cashing out and other departments, every department form the attachment whose core layer is close, outside is loose under the direction of ringleader. Different from traditional group crime, attacking cloud storage platform and other related cybercrime presents the situation of online crime major, offline crime complementary, elements of constitution of crime group diluting and other traits, bringing big difficulty of drawing evidence, trouble of applying to law and other problems, which results in the outstanding contradiction of imputation in penal cases, social harm not matching with legal response ultimately.

**Variation of Characteristic of Group Crime**

During practice, investigative organization adopts crime group theory to carry out the cognization and investigation of crime according to the condition of solving cases together. However, unlike traditional drugs and group crime with gang and evil, group crime of network space has its own features, for example, low cost of building organization system, high liquidity of personnel, flexibility of criminal intent conveying and other traits, which not only enhance the number of such kind of group crime sharply, but also increase the difficulty of emputation.

It is traditionally believed that, group crime is a specific crime pattern of joint crime, therefore it must satisfy the elements of constitution of joint crime. Nevertheless, there are two kind opinions about concrete understanding of network group crime. The broad one starts from the angle of damaging result, using dangerous crime as perspective, thinking that more than three actors use CNT (Computing Network Technology) to carry out criminal behavior, if causing substantive harmful effects, it can be defined as Internet group crime. [7]Narrow sense starts from the angle of mode of behavior and objects, thinking that only crime objects and criminal skills networked belong to Internet group crime. [8] In practice, to No285,286,287 pieces of criminal law, namely crime which criminal law applying to network stipulates as traditionally considered. Generally speaking, theory of interpretation evades different opinions towards network group crime theoretically. Taking No285 of criminal law as an example, practice department starts from the angle of object, the perspective of crime pattern, considering crime which the first piece stipulates only have accomplished and unaccomplished two forms. Crime the second piece stipulates only has accomplished form while the third piece is the stipulation of accessory’s outing. Such understanding belongs to the scope of interpretation theory essentially which the inside of criminal law system controls. However, to attacking cloud storage platform and other related network crime, its process of committing a crime is extremely complicated, I will try to inspect this process from the angle of group crime.

Group crime is a special form of joint crime, but it still focus on the meaning of accomplice. [9]Therefore, attacking cloud platform and other cybercrime can be divided into two types with the standard of having or not having common criminal intent. “Fraud cases which Peng Zhonghai, Wang Qiaoqiao, Guoyanyan involved” can be considered as an example in the former one. In this case, Liu Liang and other people gained citizen’s personal information and then sold it to Peng Zhonghai to
carry out telecom fraud by copying secretly, buying from other people and other illegal ways. This case belongs to group crime, but presents the characteristic of elements of constitution weakening, the sense of accomplice concealing, complicity relation divided and others. In the determination of crime, we follow the fundamental theory of joint crime generally.

In this case, by combining the fundamental ideas of implicated offense, we are able to determine the crime of Peng Zhonghai and other suspectcs who buy citizen’s personal information, which means that we consider “purchasing” as the means of criminal, “defrauding” as criminal purpose. Therefore we follow the general theory of “choosing a felony to penalize implicated offense.” To Liu Liang and other actors who sold citizen’s personal information, we should consider the principle of “choose a felony to punish imaginative jointer of offenses” according to criminal intense.

However, in the same kind of cases, there are still some debate about whether we should impute it to the crime of invading personal information and computer crime in judicial practice. To state this issue, I made chart 1 to elaborate.

Table 1. The Statistics of Typical Cases of Cyber Crime Which Are Related with Cloud Storage Platform.

<table>
<thead>
<tr>
<th>Date</th>
<th>Basic condition of case</th>
<th>Legal consequence</th>
</tr>
</thead>
<tbody>
<tr>
<td>The case of Yang Renqiang defrauding and invading citizen’s personal information in Henan Puyang in 2016</td>
<td>Yang Renqiang and Tan Shengxin. After Tan’s premeditation, he decided to use QQ to defraud. Afterwards, Tan Qimin joined. Yang Renqiang and Yang X purchased and stole citizen’s personal information, with which to steal other’s money.</td>
<td>To Defedent Yang Renqiang, several crimes are carried out together, therefore imprisonment, and deprived of political rights lifetime and fined. Recover illegal income of Yang and return it to victim, HeNan JuFeng bio-energy developing limited company</td>
</tr>
<tr>
<td>The case of Peng Zhonghai and Wang Qiaoqiao defrauding in Sichuan Guangyuan in 2016</td>
<td>Peng Zhonghai first mastered the way to defraud and wooed personnel who have the experience of defrauding, then use the way of paying cash on delivery to cheat victims’possessions. After buying lots of citizen’s personal information, Liu Liang, Liukai and Ye Mengjiao sold them to Peng through QQ account.</td>
<td>Repealing the first item which SiChuan guang yuan intermediate people’s courts, Peng Zhonghai committed the crime of defrauding, and sentenced to fifteen years in prison, at the same time, Peng and other appellant were fined half a million and detained on housing and funds.</td>
</tr>
<tr>
<td>The case of Xie X chao and Huang X jia defrauding in Guangdong Maoming in 2015</td>
<td>Defendants Huang X Jia, Lei X Yi, Huang X Yi and Huang X Bing, Shao X, Li X dialed telephone defrauding, ignoring country’s law. Defendants Xie Xchao, Huang Xding helps associates to draw filthy lucre defrauded</td>
<td>Xie Xchao, Huang Xjia, Huang Xyi, Li X, Huang Xbing, Shao X and Huang Xding commited the crime of defrauding, recovering illegal income which were defrauded of Xie and Huang Xding, returning it to victims Pan</td>
</tr>
<tr>
<td>Case Description</td>
<td>Details</td>
<td>Party</td>
</tr>
<tr>
<td>---------------------------------------------------------------------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------</td>
</tr>
<tr>
<td>The case of Wu Shujiang and Wang X defrauding in Fujian, Anxi in 2016</td>
<td>Wu Shujiang employed defendants Wang X and Chen Zhengen to acquire information of disabled illegally, then posed as the workers of DPF center, tricking victims into taking bank cards to operate on ATM and cheating them of money.</td>
<td>Wu Shujiang committed fraud crime, the crime of invading citizen’s personal information; Wang X committed fraud crime, recovering the illegal income of co-defendants to turn over to the state treasury, confiscating Wu and Wang’s crime tools which were detained.</td>
</tr>
<tr>
<td>The case of Zhang XX and Yao XX gaining citizen’s personal information illegally in Shanghai Huangpu in 2016</td>
<td>In the condition of lacking the authorization of the website, Zhang XX entered operating background system of this website, acquiring the information and sold it to Yao xx, Yao xx increased price to resell for profit in Internet after purchasing the order information.</td>
<td>Zhang XX and Yao XX committed the crime of invading citizen’s personal information, being sentenced to in prison with fine. The crime tools detained were confiscated, recovering the illegal income of Zhang and Yao.</td>
</tr>
</tbody>
</table>

**The Creation of Network Criminal Law is Insufficient**

Information Internet technology has developed from Web1.0 to Web3.0, the reflection thinking of criminal law has jumped from “software thinking” into “network thinking”. The revolution of reflection has brought the reformation of penal legislation system whose core is four unmixed cyber crime *Criminal Law amendments (Nine)* stipulates. So, our criminal law opened up a specific area, namely network criminal law towards which the reflecting pattern of education field can be divided into lawmaking theory and explanation theory.

Lawmaking theory claims that “Two tracks, Three points, four lines” response pattern is not enough to reply to the complex crime pattern of cybercrime, hoping that we will build brand-new system of accusation when aiming at cybercrime. [10] Explanation theory claims that scholars of criminal law should jump out of the box of legislative centralism, focusing on internal controls of systems of criminal law emphatically. [11] I deem that the common ground

Using the view point of people who advocate legislating to evaluate the imputation mode of our legal system towards network society, there are “Two tracks, three points and four lines” criminal
response pattern and network legal system with constitution at the lead, criminal law, social law and civil law system interacting with one another, however, there still exists the problems of single focus of criminal law, difficult criminal responsibility, network thinking delaying, qualitative and quantitative criterion lacking, which will result in the delaying of response reaction system.

**The Object Regulated by Criminal Law is Single.** Aiming at pure network crime, the focus of our criminal law is software, system, data, exhibiting concretely in No 285,286,287 piece of *Criminal law (Nine)* which are added newly. The revision of this three piece marks the arrival of our network criminal law, forming the trunk of our network criminal law with *The decision about Internet safety*. No.285 piece protects national affairs, defense construction and other data of computer information system which are related with national profits, the second item is the interception and added item of first item, in the meanwhile, the third item is designed to strike actor, these three are unified in striking the behavior of gaining computer system data illegally, however, No.286 and No.285 are both protecting the data of computer information system. No.287 piece is the addition of No.286 and No.285, realizing the difference between computer crime and Cyber Crime, it focus on attacking actors. In the relationship of three, Criminal activity which No.285 and No.286 describe are both the behavior of using computer as criminal tool, besides, they merely protect computer information system, these rules are the reflection of Cyber Crime instrumentalizing. In practice, No.286 and No.285 pieces are higher than No.287 piece in legal status. Nevertheless, in Web2.0 age, No.287 piece, which will become the qualitative criterion of traditional crime networked appears more important ever since.

**Criminal Punishment Lagging.** The Internet Alienation phenomenon of crime exists widely in traditional crime networked. Taking form of crime as an example, there exists the problems of illegal properties of preparation action alienating, having difficulty in differentiating accomplished from unaccomplished, the way of evaluating lacking at the stage of suspension. As far as preparative behavior is considered, there exists huge difference between it and traditional crime in the boundary between preparative and practical behavior and causality between it and damaging results. Based on this thought, judicial practice enhances the strength of penal imputation at Internet crime prepared stage. However, in theory, punish ability of preparative behavior is limited by the legitimacy of legal principle, necessity of penal policy, uncertainty of origin of assessment of preparative behavior. The punish ability in preparation stage of cybercrime is derived from chained developing tendency of telecom fraud cases in penal policy, specially after Aug.19th , Xu Yuyu Case, practice department will consider attacking the origin of information given away as the key to investigate cases, nevertheless, in specific penal punishment, the problems which the guilty of people who give away information are consistent and penal punishment is front are overlooked, resulting in the consequence of the origin which leads to crime not removed. In theory, the essence of this problem is whether we are clear about the timing of penal punishment. The timing of penal punishment is crime itself rather than accomplished crime originally, therefore, better to think the punishment to accomplished criminals is followed than think punishment to unaccomplished criminals is front. In conclusion, in the age which cloud storage technology are developing quickly, to strike some crime related, we should possess thoughts of crime collectivizing, hoping that we can figure out who is responsible for this through whole train. At the same time, in attacking preparation criminals, we should reject traditional thoughts and carry out exceptional punishment.

**The Obstacle of Penal Imputation.** Immediacy and high technicality of Internet technology determine that cybercrime requires joint crime to achieve the purpose of committing crime. According to traditional theory of joint crime, there exists three reasons why it is difficult to carry out the imputation of cybercrime:

Traditional crime theory requires behavior demands that actor possesses the consensus of committing crime, they not only have common criminal purpose, but also have definite meaning connection. However, in practice, crime of attacking cloud storage platform and other related cybercrime are more likely to belong to unidirectional meaning connection. Attackers see attacking cloud and database as their jobs, acquiring huge number of citizen’s personal information extensively.
Although they know clearly that the data they sell will be used to commit other cybercrime, they still sell them to the third man to commit other cybercrime. According to general joint crime theory, this relation cannot be demonstrated as joint crime. Nevertheless, based on related judicial explanation, data provider should be punished as user committing joint crime. Therefore, there exists large contradiction between penal theory and judicial practice, and there are logical insufficiency in legal principle. [14]

According to traditional conviction and sentence theory, we consider principle offender as basic gist of conviction and sentence, while the punishment of abettor are determined by whether helping behavior is major or not. However, for attacking cloud platform and other related cybercrime, taking spreading pornographic materials to gain profits for example, this theory can easily cause the results that criminal involvement is not consistent with criminal punishment. Although Internet operators know clearly that storage platform storing pornographic materials is easily attacked, they still store plenty of pornographic materials which leads to further spreading of it. In this kind crime, Internet operators provide and spread plenty of pornographic materials in form. However, in essence, attackers has dominant status in the process of spreading pornographic material. In such condition, no matter we determine who as principle offender, we are all face the query of criminal involvement theory.

Non-national boundary of cybercrime makes nation jurisdiction of cybercrime imputation the understanding contradiction. In this problem, only Budapest Cyber Crime Convention has related rules about this contradiction, but this pact is very different from present criminal law. Therefore, China didn’t accede this treaty actually, which led to the result that we can’t start criminal accounting and booty recovery of foreign cybercrime problems. In practice, taking telecom fraud as an example, China can only talk to operators, pockets, riders and other actors who belong to second criminal circle to start criminal accounting. However, to attackers who gained data of citizen’s personal information and other actors who belong to first crime circle, we can only carry out attributing crime by deviating from territorial and personal principle of non-national boundary characteristic.

**Criminal Law Response**

Facing joint crime characteristic varying, illegal properties alienating, sum of crime increasing sharply and other practical sin, we find that current Internet criminal law creation insufficiency which reflects in focus of criminal law single, network thinking lagging, which led to criminal imputation obstacle. Aiming at this, in the face of legislative expanding and complex sin, how to accurately define relation of right and obligation among people who involved in attacking cloud storage platform and other related cyber crime becomes the premise of criminal imputation.

**Guiding Philosophy**

Internet development of our country experiences approximately three innovations: commercial innovation, institutional innovation and cultural innovation. (see chart 2) [15] However, at the same time, crime also gradually develops to the stage where traditional crime and network crime overlap, as shown in the table.

<table>
<thead>
<tr>
<th>Stage names</th>
<th>Prehistoric period</th>
<th>First stage</th>
<th>Second Stage</th>
<th>Third Stage</th>
<th>Fourth stage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Stage properties</td>
<td>Science phase</td>
<td>Commercial stage</td>
<td>Social stage</td>
<td>Real-time stage</td>
<td>Network space stage</td>
</tr>
<tr>
<td>Outstanding properties</td>
<td>Academic feature</td>
<td>Media property</td>
<td>Socialization property</td>
<td>Real- time property</td>
<td>Network space property</td>
</tr>
</tbody>
</table>
The shifting of crime requires the foundation of brand-new penal legislation and thinking mode, however the tendency should be the battle between mixed legal interest. People who agree with protecting legal interests think that there exists interests which are nature or built by it, such as protecting life and legal properties from invading, preventing social order from destroying and so on in criminal law. [16] Nevertheless, we still need to consider the limitation, category and immutability, priority and others of protection if we are in support of protecting legal interests of criminal law. In guiding ideology, to cybercrime, we shouldn’t consider personal and social interests which is better as taxonomy. On the contrary, we should build and formulate brand-new concept of legal interests protection aiming at new-type crime form. [17]

To be specific, first, attacking cloud platform and other related cybercrime are fused with generic characteristic of cybercrime and traditional crime. The evaluation of this kind of crime will cross the different chapters of current criminal law, involve different kinds of legal interests, which will be difficult to assess based on current items. Therefore, we ought to give up traditional side-by-side legislation model, legislation structure of thinking integration. That is, basing on a series of criminal chain and mode, considering a series of sin and judicial explanation, taking a series of measures which criminal law stipulates. Second, when building quantitative standard system concretely, we should jump out of shackles of traditional quantities crime theory. Traditionally, condemnation amount of quantities crime includes financial loss sum, illegal gain sum and illegal management sum three meanings. [18] Taking these three meanings as typical cases, after careful analysis we can find that if we see quantities crime as our perspective, the attacking of criminal law to cloud storage platform are based on capital flows, then strikes consequently, as chart 6 showed.

Although the standard of conviction and sentencing which this leads to can satisfy the need of evaluation of normal accomplished crime in information age, there isn’t corresponding standard of conviction and sentencing in the problems of joint crime, crime attempted, abettors and principal offender. To this, writer thinks that quantities crime theory in cloud age should have some development and carry out revolution based on two-way cognizing criterion of criminal amount. First, to abettors whose crime amount is large in joint crime, we should divide standard of amount of principle offenders. Second, suspects who provide technical support for other cybercrime suspects and cause actual harmful result, his criminal earnings should be reckoned in joint criminal earnings. Third, people who help other cybercrime suspects cash should be convinced and sentenced according to the sum.
Responsibility Division

Attacking cloud storage platform and other related cybercrime belong to new-type crime, but it can’t be independent of traditional crime. As a complex criminal pattern, it possesses responsibility of accomplice, responsibility of principle offender and responsibility of platform. In practice, it can be divided into responsibility distribution system of “unidirectional three-circle number group” according to crime patterns, as figure 7 shows. Subjects who control information grasp a lot of citizens’ personal information, relying on its industrial advantage status. However, the responsibility it takes and rights it possesses are not balanced. Other cybercrime behaviors takes advantage of concealment and unipolarity of territory to make malconformation and unbalancedness and among crime cost, legal interest violation and crime benefits highlight. Criminal gang cashing appears the characteristics of large-scale and systematism, facing the obstacle of penal imputation.

Rights Limitation of Subjects Controlling Information---In the Perspective of Responsibility of Accomplice. Using the relevant analysis model of SPSS, we carry out the bivariate correlation analysis of number of invading citizen’s personal information crime from Jan. to Jun., 2018 and number of all kinds of cybercrime network security incident from Jan. to Jun., 2018. From this, we draw a conclusion that, pearson correlation coefficient between number of invading citizen’s personal information crime and number of all kinds of network security incident is 0.596, and the data is calculated by these six sample data, its actual significance level is 0.212. Considering the error of searching data, the actual data are not very different from the theoretical data, which can explain that value of coefficient of association is not caused by casual factors. 0.596 is greater than 0.500, stating that there exists a positive linear correlation between invading citizen’s personal information crime and all kinds of cyber network security incident as figure 8 shows. We can obtain further that the protection efforts to citizen’s personal information from information controlling subject and the happening of all kinds of network security incidents are in positive correlation.
Guided by this, combining with practice, to stealing information online crime which is supported by hacker technology, our criminal law makes prohibiting stipulation in the way of negative list, however, the stipulation of obligation and division of powers to the information controller are not balanced. To duty crime which selects mole as model, we execute punishment according to the duty crime and invading citizen’s personal information crime. Nevertheless, it often causes result in which guilty inconsistent.

The focus of above-mentioned contradiction is the different understanding of whether “conducting criminal” and “participating criminal” form which is in joint crime system model is adapted to current criminal. Therefore, we should carry out analysis of system appearance and system connotation which we should think about when we design joint crime theory to solve problems of “participating criminal” form. First, in the perspective of system appearance, we should make special provision of the incriminating standard and punishment principle of “participating criminal” form in the general provisions of criminal law. If we use specific provision of criminal law to forgive “participating criminal”, it will impair the gist of convicting principal offender and break “participating criminal” typification thinking. In Taobao service personnel defrauding case, if we are guided by this direction, information providers who are considered as “participating criminal” are not only convicted of invading citizen’s personal information, but also the joint crime of defrauding. At the same time, the condemnation amount will be the same as “executing criminal”. Second, in the perspective of system connotation, the bound between “participating criminal” and “executing criminal” is differentiated strictly, meanwhile, they are alienated observably in behavior connotation and obligation gist. In the relationship of “participating criminal” and “participating criminal”, all the contribution to the corpus delicti and its illegal connotation all possess cocategorical value. [19]Therefore, there is no need to define excessively the limitation between “participating criminal” and “executing criminal”.

In the perspective of joint crime theory, combined with Britain new Data Protection Act, we have following suggestions. First, we should add “distinguishing” system to general principle and implement “partly carrying out and take all” principle into specific provisions. In Anglo-American Legal system, the legislation of joint crime which mainly establish the condition off punishment on the basis of criminal liability principle of attempted crime and narrow joint criminal, belongs to former. [20]Second, using New Data Protection Act as a reference, we should expand citizen’s rights to control their own information to narrow data controller’s rights to use information. For example, in “informed consent” system, we focus more on “citizen agreeing” and we require that this agreement should be “clear and easy to backout”. In the same time, we should stipulate” rights to be forgotten”, and citizens have the rights to request that information controller delete personal data. To government agency’s rights to gather information we should specifically stipulate that government agency ought to reduce the behavior of gathering information repeatedly. Meanwhile, we can timely post the dynamic of government in portal website in order to make it convenient for citizen to know about their own rights.

**Responsibility Assigning of Other Cyber Crime Actors.** In practice, the condition of high incidence of cybercrime requires that punishment should expand, in order to follow the principle of
statutory principle, we should further explain principal offender theory. Considering “limited principal offender” as viewpoint, principal offender is the person who use his own body movements to directly satisfy elements of constitution, [21] which means that in joint crime, except for principal offender, other participates are all the joint offenders. However, this opinion will easily cause typed thought and expand the range of penal punishability without limit. Therefore, how to explain principal offender theory should consider defining responsibility assigning will be influence by criminals to what extent as the first factor to considerate.No.2,3,4,5 item in No.33 piece of Russian penal law made a clear concept of conducting criminals, organizing criminals, abettors. In the aspect of assuming concrete responsibility, No.34 piece erases the problem, stipulating the responsibility of every participates during the crime are determined not only by its degree of participation, but also by its property of conducting crime. This makes it clear that in joint crime, the responsibility of participating criminals and principal offenders should be distributed by participating property and distinctions and functions of damaging results. The understanding of our penal law of principal and participating criminals is focused on considering contribution degree, causing the embarrassing result of low contribution degree and high harm degree in some telecom fraud crime. Taking POS fraud, encashment and cashing case as example, the means of criminals to escape from striking are impossible to defend effectively, they consider achieving drifting out of incriminating standard as goal. Therefore, if we consider property and real damaging effect conjunctively, we can carry out assuming according to the incriminating standard of principal criminals.

To sum up, to penal imputation of cloud crime, we can roughly carry out designing from the angle of guiding concept and responsibility division. Focusing on concept of protecting legal interest, incriminating standard, narrowing information to control rights of subject, deploying responsibility of other cybercrime behaviors and others to reform current legislation system.

Summary

During the forty year of reform and opening -up, our Internet technology develops rapidly. Facing worldly affairs and sin, penal law made the effort to strike cybercrime artificially and build reaction system of cyber penal law which possesses Chinese characters. However, to attacking cloud storage platform and other related cybercrime, we still haven’t reach the level of solving all the contradictions. The prospect is bright but the road is winding. In the process of searching the way of settling, we should firstly clarify the process of crime, considering following the line to strike, at last, we can realize that every circle can be affirmed, everything can be accounted. Secondly, we should exhaust the legal principle behind the problem in order to focus on the problem. At last, we should insist on the guide of the problem and try to commence guiding concept, then think about the thinking path of new crime-new thoughts-new theory. In the end of this article, we are glad to see that Ministry of Public security has carried out the new round specific activity of attacking and governing new type of cyber crime, which is laudable without doubt. At the same time, NPC has added the legislation of Personal Information Act to the legislation plan, which will be sure to strike the tendency of cybercrime which is of precision, in the same time, the process of variation will lag. However, the reform has accessed the deep end, opening-up will be all-round and go into more fields. Therefore, whether the following forty years’ related crime will Europeanized and present the character of internationality still need further thinking and efforts of legal theory researchers.

References


[2] See also Cameron Chapman:” Internet history (1969-2009)”, jcky translate, http://article.yeeyan.org/view/435041/70880? from = timeline&isappinstalled=0. Latest visit date: March 5, 2019. See the original text Cameron Chapman:” The History of the Internet in a


