Cases Study and Analysis of the Court Judgement of Cybercrimes in Taiwan

Jai-Rong Sun¹, Mao-Lin Shih², Min-Shiang Hwang¹*

¹ Department of Computer Science and Information Engineering, Asia University
² Department of Financial and Economic Law, Asia University
* Corresponding author: mshwang@asia.edu.tw

Abstract— with the development of information technology and Internet, the criminal model have been changed. The Internet has become an instrument of crime as a new type of criminal means, which is called cybercrime. There are different implementation techniques between common Internet crime and traditional crime. The court-judgement based on the evidence for the Internet crime has also changed compared with the traditional crime. The main litigation proceedings taken by the judge between the cybercrime and traditional crime are slightly different. In this paper, we analyzed the common cybercrime by using actual court-judgement results in Taiwan, and then generalized the common evidences of cybercrime. Finally, we compared the litigation processes between traditional crime and cybercrime. It is hoped that judicial court-judgement for the cybercrime will be more cautious so to prevent the occurrence of misjudgement.

Keywords—Cybercrime, Digital evidence, Cybercrime judgement

I. INTRODUCTION

In recent years, the development of information technology and Internet has increased convenience in people's lives. However, many social problems have happened in Internet, even including criminal acts. In the criminal codes amendment of Taiwan, the computer crimes have two aspects, broad sense and narrow sense. The computer crimes using computers or Internet equipments are belong to the broad sense; the narrow sense of computer crimes are means the acts which target to attack computers and Internet. In this paper, we opine the cybercrimes [13] belongs to a kind of computer crimes, and it's an illegal act by using computers or electronic equipments to connecting Internet from wireless or wired network.

In fact, if the perpetrator uses computer to commits the traditional crimes on Internet, the traditional crimes act will be called the cybercrime. For example, the perpetrator commits traditional crimes act by using wireless, VOIP (Voice over Internet Protocol), Smartphone, or Cloud to make some illegal act. About the problems of investigation and forensics in the foregoing cybercrime act has many methods be proposed, including investigation procedures [1-3, 10, 14, 25], the ways of collecting digital evidences [7, 9, 20], and the ways of identifying digital evidences [4, 21, 24]. However, when the cybercrime cases are transferred to the court, the digital evidences and litigation procedures will become the keys for the court judgements of cybercrimes.

Cybercriminal types not only be included in the chapter 36 of Taiwan's Criminal Code, but also has other tradition criminal acts types, such as verbal abuse, sending threatening letter, or breaching copyright. If the perpetrator through the use of a computer connected to the Internet carry out criminal acts, it will make the traditional crimes become the cybercrimes. In this paper, we describe the common cybercrime and actual court-judgement results in Taiwan, and then generalize the common evidence types of cybercrime. After this, we propose a cybercrime selection method used for court judgements to collect the judgements into our statistics data, and compare as well as analyze the statistics results. At last, we compare the litigation processes between traditional crime and cybercrime. The remainder of this paper is organized as follows. In Section 2, we describe the common cybercrime in Taiwan. Section 3 analyses the standard of proof as well as the main types of evidence from cybercrime court-judgements. In Section 4, we propose a cybercrime selection method for court judgements, and use this method to compare and analyze the statistics results, including common evidence types and digital evidence types. In Section 5, we compare the litigation processes between traditional crime and cybercrime. Finally, we draw our conclusions in Section 6.

II. THE TYPES OF CYBERCRIME

In Taiwan, the criminal law follows a legal principle called “Nulla poena sine lege (No penalty without a law)”, and it means when people do something that is not prohibited by law, they cannot be punished. On the other words, this existing criminal law is a narrow and clear concept with high immutability, and the features will provide clear and stable rules for every people. The purpose of this legal principle is used to protect people's freedom, and avoid them to suffer unreasonable punishment. This legal principle is also applicable to cybercrime types. Hence, according to the cybercrime reports of Taiwan Nation Police Agency [17] and the cybercrime court-judgements of Taiwan, the common cybercrime includes Against Reputation, Fraudulence, Against Morality, Infringe IPR (Intelectual Property Right), and Against the Computer Security.

A. Offences Against Reputation of the Internet

Against Reputation contains insult and slander in public place. In the cybercrime, the insult and slander publicly
The Infringe IPR contains Patent Act, Trademark Act and Copyright Act. In 2001, the Patent Act has abolished penalty in Taiwan, and changed the way of solving the problems of patent's tort to civil procedure. The cybercrime of Intellectual Property Rights on the Internet consists of infringe trademark and infringe copyright [15]. We will describe the infringe trademark of cybercrime and the infringe copyright of cybercrime as below.

1) **Infringe trademark of cybercrime:** Infringe trademark of cybercrime means that the perpetrator without proprietor consent, and uses a trademark which is similar to the registered trademark or collective trademark on the goods, and then sells, possesses, displays, exports, or imports through electronic media or on the Internet.

2) **Infringe copyright of cybercrime:** Infringe copyright of cybercrime consists of illegal reproduction, public infringement, illegal disseminates and displays. In the cybercrime of infringe copyright, the perpetrator uploads and downloads the reproductions without the copyright holder authorization, or displays as well as sells the reproduction object publicly through website of trading on the Internet.

### E. Offenses Against the Computer Security

In the 2003, In order to prevent and punish the computer crime, there has increased a new chapter 36 in Taiwan Criminal Code—Offenses Against the Computer Security (OACS). The criminal act of this chapter belongs to narrow sense of computer crimes, and the objects of crime are computers or networks [29]. The OACS includes Act 358—illegally accesses another person's computer, Act 359—illegally deletes or alters the magnetic record of another's computer, Act 361—illegally interferes another's computer, and Act 362—makes the malicious programs. In the 2012 from January to August, there had total 3,342 cases of OACS in Taiwan. The Act 358 had 1,514 cases, The Act 359 had 1,568, and the others had 260 cases [16]. Thus, the main cases of OACS are massive in Act 358 and Act 359, and we will describe the Act 358 and Act359 as below.

1) **Act 358—illegally accesses another person's computer:** The legislative purpose of this code is to punish the perpetrator without reasons embezzling another's account as well as password, or breaking his computer protection, or taking advantage of the system loophole [19], and causes serious injury. Therefore, this code objective needs some basic conditions: first, the perpetrator without reason; second, entering another's account code and password, breaking his computer protection, or taking advantage of the system loophole; finally, this act will be causing injury to others people.

2) **Act 359—illegally deletes or alters the magnetic record of another's computer:** The legislative purpose of this code is protecting the digital or virtual property, and avoiding the digital data of user's computer will be alter, delete, or damage. Therefore, this code objective needs some basic conditions: first, the perpetrator without reason; second, deleting or altering the magnetic record of another’s
computer or related equipment; finally, causing injury to another person.

F. Offences of Gambling on the Internet

In the offenses of Gambling, there must have gambling at a public place or the place open to the public. Called the place of gamble, it just needs a place to gamble enough, and doesn’t limit in entity places. In recent years, the messages of gamble are transmitted by telephone, fax, or Internet. Thus, the perpetrator of gamble acting on the Internet builds a gamble website, where let another person connect this website to gamble each other, and then gets profit by this website.

III. THE TYPES OF DIGITAL EVIDENCE

The Digital Evidence [23] is generated by development of computer and Internet. It is used to prove the fact of crime exists or not, and the level of correlation between the perpetrator and the fact of crime. The Digital Evidence includes text (word) data, digital video, digital figure, program, electromagnetic record, and the others digital data stored at computer device. Since the digital data is stored at a computer device for binary electronic signals, it not belonging to entity evidence, and cannot be understood directly. For this reason, the information of digital evidence presents the contents necessarily through translation and compilation. According to the above-mentioned description for digital evidence, it has some characteristics shown as below [23].

- Not easy to collect and preserve
- Easy to copy and modify
- Not easy to prove the source and integrity
- Not easy to understand directly
- Not easy to build the relevance

According to the Taiwan crime code 165-1 II , digital evidence is a new type of evidence. The definitions of digital evidence in Taiwan are described as below: the crime code 10 VI, “The term electromagnetic recording means records for computer process made through the use of electronic, magnetic, optical or other similar means.”; the crime code 220, an audio recording, a visual recording, or an electromagnetic recording and the voices, images or symbols that are shown through computer processes with sufficient evidence of intention shall be considered a document. The Electronic Signatures Act code 2 I, “electronic record means a record in electronic form, which is composed of any text, sound, picture, image, symbol, or other information generated by electronic or other means which are not directly recognized by human perceptions, and are capable of conveying its intended information.” Therefore, the digital evidence has been defined clearly in Taiwan law.

The way of common classification at digital evidences is described as follows [5]: printable and non-printable, analogy and digital, original and copy, automatic generation and anthropogenic [6]. In this paper, we collect the court-judgement s of recent years, and we divide the common evidences into the following types: Computer Log Records (CLR), User Register Data (URD), and Behaviour Fact Data (BFD). The CLR is a digital records generated automatically from a computer and other devices [6], for example, IP (Internet Protocol) address [18], MAC (Media Access Control) address [8], website login records, electronic transaction records, game course records, and Current Research Information System (CRIS) of Internet Service Provider (ISP). The URD is users’ personal information when they apply for the account on the Internet, or rent the connection device of Internet. The URD is stored on the database of the ISP, and it has relevance between applicants and accounts, for example, register data of account, register data of website, and the Internet user’s data of register as well as application. The BFD is a kind of evidence stored at the computer and other devices, and it will be used to prove whether the behaviour is a crime or not, for example, the figures and words of website, electronic document data, program, and communication and short massage record. Besides, there are two elements will affect the result of court-judgement, Accused Confession (AC) and Material Evidence of Seizure (MES). AC means that the perpetrator admits or describes the crime fact, and it must be under the freedom as well as the legal procedure. MES means that the material evidences are related to crime fact from searching and distraining by judicial policemen, for example, data storage of computer device and contraband. The evidence types of cybercrime court-judgement are shown in TABLE I.

<table>
<thead>
<tr>
<th>Evidence types</th>
<th>Evidence Source</th>
</tr>
</thead>
<tbody>
<tr>
<td>Digital Evidence</td>
<td>CLR, ex. IP address</td>
</tr>
<tr>
<td>Evidence</td>
<td>URD, ex. register data of account, register data of website</td>
</tr>
<tr>
<td>AC</td>
<td>The perpetrator admits or describes the crime fact</td>
</tr>
<tr>
<td>MES</td>
<td>Data storage of computer device and contraband</td>
</tr>
</tbody>
</table>

IV. THE COMPARISON AND ANALYSIS OF CYBERCRIME COURT-JUDGEMENT RESULTS

In the criminal procedure of Taiwan, the probative value of evidence is based on the firm confidence of the court, and it not be allowed to violate the rules of experience and logic. Thus, the probative value of evidence is the source used to let the judge determine an inner conviction. Due to no evidence no crime, the evidences must be investigated legally first, then it will be has the probative value, proving whether the crime fact exists or not. However, in the cybercrime, the perpetrator commits the crimes via using a computer and others devices to connect Internet to hide himself, so he does not get in contact with the victim directly. Furthermore, the digital evidence is easy to copy as well as modify [23], and there still has misgiving in how to confirm the relevance between a perpetrator and the crime fact.

In this paper, we use a selection method to select the cybercrime case of Taiwan from Law & Regulations
This selection method for court judgements is used to collect the court judgements about cybercrime, and compare as well as analyze the difference between the traditional crime and cybercrime. Since using Internet needs an IP address, and the cybercrime is a crime which has happened in Internet, the cybercrime must be correlated with IP address. However, the criminal case correlated with IP address does not represent the crime scene happening in Internet. Therefore, if the criminal case has happened in Internet, and the perpetrator also has committed the crime by using a computer, this criminal case is called cybercrime. Consequently, in this selection method, we define three conditions to confirm whether this case belongs to cybercrime court judgements: First, determine whether correlated with IP address; second, determine whether correlated with Internet; third, determine the types of court judgements results including finished and unfinished judgements. The finished judgement means the result of judgement is either guilty or innocence; the judgement of unfinished is mean the result of judgement be transferred to the other court, or indictment be rejected. When a court judgement meets the above all conditions, this judgement will be collected into our statistics data in this paper. The steps of selection method are:

**Step.1 Start to select:**

In this state, the court judgement will be selected out from Regulations Database [22]. This court judgement will be confirmed by the Steps 2-4 as below.

**Step.2 Determine the correlated with IP address:**

By confirming the correlation with IP address, we determine the defendant has ever committed the criminal case via using computers in this court judgement. This computer must have a virtual/fixed IP address.

**Step.3 Determine the correlated with Internet:**

The correlation with Internet means the criminal case has happened in Internet. This stage is used to confirm whether the criminal case has happened in Internet via examining the verdict context.

**Step.4 Determine the types of court judgement Result:**

The types of court judgement result will present it's either a finished judgement or an unfinished judgement.

**Step.5 Select Again:**

If a court judgement does not have all conditions of Steps 2-4, we will select the other court judgements again, and determine whether the judgement meets the above conditions or not.

**Step.6 Accumulate the Finished Judgements:**

In this stage, we will collect the court judgement which meet the above conditions of Steps 2-4, and accumulate the statistics data of this paper.

In the court-judgements of cybercrime, there are total 196 finished judgements including the innocent or guilty judgements. There have 183 guilty judgements, 13 innocent judgements, and 13 other judgements. The result is shown in Fig. 2.
According to Fig. 3 and Fig. 4, the most evidence belongs to digital evidence in cybercrime, the second is AC, and the least is MES. In the digital evidence, the most is BFD, the second is CLR, and the least is URD. Therefore, when the court determines the cybercrime, the first consideration is digital evidence. The BFD, CLR, and URD are used to confirm who is the perpetrator and what is the crime fact; then AC and MES are considered to determine firm confidences. In the court-judgements of traditional crime, witness and perpetrators’ testimony are used to confirm the crime fact, and the material evidence and document evidence are used to prove perpetrator is guilty or innocent. Thus, in the traditional crime and cybercrime, the evidences which effect court-judgements result are different.

V. COMPARE THE COURT JUDGEMENTS BETWEEN CYBERCRIME AND TRADITIONAL CRIME IN LITIGATION PROCEDURES

According to the Taiwan Criminal Procedure, We divide the cybercrime litigation procedures into two types, regular procedure and non-regular procedure in this paper. The regular procedure (also known as normal judiciary procedure) has oral arguments, and the non-regular procedure doesn’t have oral arguments. The non-regular procedure includes Summary Judgement Proceeding and Summary Procedure. There are total 264,367 criminal court-judgements at the first instance of district court in 2011. In the total court-judgements, there have 167,631 judgements that have judgement ended at the first instance of district court [11] (doesn’t include non-regular procedure), accounting for 63.41% of all the judgements; the non-regular procedure have 96,736 judgements at the first instance of district court [12], accounting for 36.59% of all the judgements. In this paper, there totally have 196 cybercrime court-judgements, 79 judgements of regular procedure at the first instance, accounting for 40.31% of all the cybercrime court-judgements, and 117 judgements of non-regular procedure at the first instance, accounting for 59.69% of all the cybercrime court-judgements. It’s shown in Fig. 5.

Consequently, in the prosecution comparison of regular procedure first instance, the cybercrime is lower than traditional crime 23.1 percentage points; on the other hand, the cybercrime is higher than traditional crime 23.1 percentage points in the non-regular procedure.

The Summary Judgement Proceeding and Summary Procedure are used to speed up the litigation process and reduce consuming the judicial resources. According to Taiwan Criminal Procedure code 273 –Summary Judgement Proceeding, if the accused admits guilty on the fact charged in the preliminary proceeding, the presiding judge may inform him of the meaning of Summary Judgement Proceeding, and decide to adopt the Summary Judgement Proceeding after referring the opinions of litigation party, litigation agent, defence attorney, and litigation assistant. According to the Taiwan Criminal Procedure code 449 I –Summary Procedure, if the perpetrator’s confession in the investigation process or other existing evidences are sufficient for the court of first instance to determine a perpetrator’s offense, the court may to announce the litigation procedure change to Summary Procedure via request of prosecutor. There has a main condition to constitute the Summary Judgement Proceeding and Summary Procedure, and it is must to obtain the confession of defendant. As mentioned above, the Summary Judgement Proceeding and Summary Procedure are used to speed up the litigation process and make defendant not need to withstand.
the pressure of litigation. However, in the cybercrime, the digital evidence is easy to be changed as well as forged, so it is not easy for the person without professional knowledge to determine whether the digital evidence is true or not. Thus, these kinds of defendants will provide hardly the advantageous or direct digital evidences in the court. Once the defendant is informed of the advantage of the Summary Judgement Proceeding and Summary Procedure, and admits guilty no matter he is guilty or not, it will causes the court to believe that the defendant is guilty.

VI. CONCLUSION

In this paper, we analyze the IP address correlated network criminal court-judgements in recent years, and sort out the common types of cybercrime, including reputation for prejudice through Internet, against property, violation of public decency, infringement of intellectual property rights, prejudice computer use, and etc. It is learned that the main evidence affecting the outcome in the cybercrime court-judgements is digital evidence, followed by the accused confession, and finally by material evidence of seizure. For the litigation procedure, behaviour fact data is most affected, followed is computer log records, and user register data is used at last. Therefore, the importance of digital evidences is still better than the accused confession and material evidence of seizure. In the litigation procedure, about the general criminal court judgements, Summary Judgement Proceeding and Summary Procedure occupy approximately 40% of total judgements. However, about the cybercrime court judgements, Summary Judgement Proceeding and Summary Procedure occupy approximately 60% of total judgements. Moreover, according to the above results, if the cybercrime case has the evidences of Computer Log Records, User Register Data, and Behaviour Fact Data, the litigation procedure has approximate 60% belong to Summary Judgement Proceeding and Summary Procedure.

The Summary Judgement Proceeding and Summary Procedure are intended to save judicial resources and avoid lengthy proceedings. According to the court-judgements results of cybercrime this paper collected, the main evidences are digital evidences from computer and Internet electronic record, and behaviour fact data. Since the digital evidence is easy to be changed and forged, it is difficult to ensure its authenticity. If the defendant has not enough professional knowledge, and the court decides to use Summary Judgement Proceeding or Summary Procedure to try this case, the defendant will not easy to provide favourable evidences to prove they are innocence in the court. Thus, to confirm and try the criminal fact, the judiciary still needs to be careful to try the cybercrime case, avoiding misjudgements.

REFERENCE
http://www.npa.gov.tw/NPAGip/wSite/ct?xItem=62452&ctNode=11393&mp=4


[22] The Judicial Yuan Of The Republic of China, Law and Regulations Retrieving System


http://jirs.judicial.gov.tw/Index.htm