Analysis of non-detectable cases of Cyber Crime Law

Jonalyn G. Nalzaro
Joan Marie Oville
College of Criminal Justice Education
University of the Visayas
nalzaroj@gmail.com

Date submitted: April 3, 2014 Date accepted: October 18, 2014

ABSTRACT

Cybercrime is emerging and it covers the limelight of today's generation. The extreme growth of new technologies has always brought solutions that aid human innovations in all aspect. But enabled criminals with complex and sophisticated knowledge to use computers in illegal ways that may result to crimes and human rights violations. The Cybercrime Prevention Act of 2012 is the first law in the Philippines that defines and penalizes cybercrimes. There are several types of cybercrimes under cybercrime law: (1) illegal access; (2) illegal interception; (3) data interference; (4) system interference; (5) misuse of devices; (6) cyber-squatting; (7) computer-related forgery; (8) computer-related fraud; (9) computer-related identity theft; (10) cybersex; (11) child pornography; (12) libel and the three cases which falls in the accomplices and liabilities of cyber criminals; (13) aiding or abetting in the commission of the crime; (14) attempt in the commission of the cybercrime; and (15) corporate liabilities. That defines the scope of its authority to exercise control within the juridical person either with or without supervision or control in committing such acts.

Keywords: *cybercrime, cyber crime act , non- detectable cases*

I. INTRODUCTION

Computers supposedly aid humans for innovations but because of drastic rate of increase of the internets and other related technologies, exercising individual rights to freedom of expression and freedom of speech, these now become an issue of abuse in morality and integrity in a national scope and go only to the nature of legislation a nation should adopt. Human rights are violated and prone to different abuses. It is therefore understandable that people are alarmed and cautious because of such cases. The undeterred prospects of arrest or prosecuting cybercriminals around the world lurk in the internet as an omnipresent menace to health, trust and emerging threat to nation's security.

The Cybercrime Prevention Act of 2012 is the first law in the Philippines which specifically criminalizes computer crime, which prior to the passage of the law had no strong legal precedent in Philippine jurisprudence. The new Act received mixed reactions from several sectors upon its enactment, particularly with how its provisions could potentially affect freedom of expression, freedom of speech

and data security in the Philippines. The difficulty on this law lies in properly defining the laws needed to allow for cybercriminals apprehension and prosecution. According to Erwin Alampay (2010) of UP-NCPAG, it is a law that is meant to protect our basic right to privacy, amidst an informational society where our personal information is collected by the state and corporate organizations. What makes this bill different is that it is framed from a rights perspective. It does not say people have new rights because of the internet, but rather, our rights must still be protected when people go online. The aspect that must be considered when we talk about cybercrime is that usually this type of criminal activities goes unpunished. It is highly lucrative and far less risky than any other ordinary crimes. The non-detected acts become a contributing factors on the increased of relative offenses concerning cybercrime.

In the current law, some areas are still unclear. Several petitions have been submitted to the Supreme Court questioning the constitutionality of the Act. There are still chances for the prevalence of Cyber Crimes considering the complexity and breadth of the virtual world. With the advent of Cybercrime Prevention Act of 2012, the researchers wanted to know what are the cases that are less detectable or cannot be detected by all means. It is also the researchers' intention to conduct an in-depth analysis of non-detectable cases of Cyber Crime Law. This will serve as key or lifeline of our law enforcement agencies to look and scrutinize deeply, in order to broaden and improve their ability in detecting and apprehending cybercrime criminals.

II. RELATED LITERATURE

Currently, there are no existing fixed literatures exploring non-detectable cases of cybercrime. Indeed, the gap between police and computer criminals is widening from time –to-time because of the enormous and advancement of cyber industry. In contrast with traditional security issues, law enforcement does not have enough experience and knowledge in ways to protect computers and networks from these kinds of crime. Thus, most computer crime incidents go undetected. Statistics on computer crime are generally not available. This is due to several reasons, such as reluctance of victims to report incidents, and uncertainty of exact definitions and classifications. Despite the absence of accurate statistics, it is generally agreed that the problem is monumental and is continuing to grow (Peters, 1997). In most cases, local law enforcement agencies do not have the personnel, equipment, and practical knowledge to proactively detect computer crime. The law enforcement community today is required to keep up with the rapidly growing use of high technology. Hence, growth of computer crime requires police officers that are familiar with advanced technology (Sen, 2001).

According to Adamski (1998) and Lohr (1997) there are incidents that cybercrime cannot be detected. The incidents that are not detected far exceed those that are detected. In essence, what is reported is thought to be only tip of the iceberg. Table 1 shows the penalized sixteen (16) types of Cybercrimes under Cybercrime Law of 2012 (Republic Act 10715):

Table 1. Types of cybercrime

1. ***Illegal access*** Unauthorized access (without right) to a computer system or application.
2. ***Illegal interception*** Unauthorized interception of any non-public transmission of computer data to, from, or Within a computer system.
3. ***Data interference*** Unauthorized alteration, damaging, deletion or deterioration of computer data, electronic document, or electronic data message, and including the introduction or transmission of viruses. Authorized action can also be covered by this provision if the action of the person resulting scope went beyond what is agreed.
4. ***System interference*** Unauthorized interference with or hindering the functioning of a computer or computer network by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data or programs, electronic document, or electronic data messages, and including the introduction or transmission of viruses. Authorized action can also be covered by this provision if the action of the person went beyond scope agreed to damages resulting stated in this provision.
5. ***Misuse of devices*** The unauthorized use, possession, production, sale, procurement, importation, distribution, or otherwise making available, of devices, computer program designed or adapted for the purpose of committing any of the offenses stated in Republic Act 10175. Unauthorized use of computer passwords, access code, or similar data are priority by the whole or any part of a computer system is capable of being accessed with intent that it be used for the purpose of committing any of the offenses under Republic Act 10175.
6. ***Cyber-squatting*** Acquisition of domain names over the internet in bad faith to profit, mislead, destroy reputation, and deprivation of others from the registering the same. This includes those existing trademark at the time of registration, names of persons other than the registrant, and intellectual property acquired with interests in it. Those who get domain names of prominent brands and individuals are priority in turn is used to damage their reputation—can be sued under this provision. Note that freedom of expression and infringement on trademarks or names of person are usually treated separately. A party can exercise freedom of expression without necessarily violating the trademarks of a brand or names of persons.
7. ***Computer-related Forgery*** Unauthorized input, alteration, or deletion of computer data resulting to inauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic, regardless whether or not the data is readable and intelligible directly, or the act of knowingly using computer data are priority is the product of computer-related forgery, for the purpose of perpetuating a fraudulent or dishonest design.

8. ***Computer-related Fraud*** *Unauthorized input, alteration, or deletion of computer data or program or interference in the functioning of a computer system, thereby causing damage with fraudulent intent.*
9. ***Computer-related Identity Theft*** Unauthorized acquisition, use, misuse, transfer, possession, alteration or deletion of identifiable information belonging to another, whether natural or juridical.
10. ***Cybersex*** Willful engagement, maintenance, control, or operation, directly or indirectly, of any lascivious exhibition of sexual organs or sexual activity, with the aid of a computer system, for favor or consideration. There is a discussion on this matter if it involves "**couples or people in relationship**" who engage in cybersex. **For as long it is not done for favor or consideration,** I do not think it will be covered. However, if one party (in a couple or relationship) sues claiming to be forced to do cybersex, then it can be covered.
11. ***Child Pornography*** Prohibited or unlawful acts defined and punishable by Republic Act No. 9775 or the Anti-Child Pornography Act of 2009, committed through a computer system.
12. ***Libel*** Unlawful or prohibited acts of libel as defined in Article 355 of the Revised Penal Code, as amended committed through a computer system or any other similar Means there are priority be devised in the future. Revised Penal Code Art. 355 states *libel by writings or similar.* A libel committed by means of writing, printing, lithography, engraving, radio, phonograph, painting, theatrical exhibition, cinematographic exhibition, or any similar means, shall be punished by prison correctional in its minimum and medium periods or a fine ranging from 200 to 6,000 pesos, or both, in addition to the civil action are priority would be brought by the offended party. The Cybercrime Prevention Act strengthened libel in terms of penalty provisions. The electronic counterpart of libel has been recognized since the year 2000 when the E-Commerce Law was passed. The E-Commerce Law empowered recognized all existing laws to its electronic counterpart whether or not commercial in nature.
13. ***Aiding or abetting in the commission of cybercrime*** Any person who willfully aids or abets in the commission of any of the offenses enumerated in this Act shall be held liable.
14. ***Attempt in the commission of cybercrime*** Any person who willfully attempts to commit any of the offenses enumerated in this Act shall be held liable.
15. All crimes defined and penalized by the Revised Penal Code , as amended, and special laws, if committed by, through and with the use of information and communications technologies shall be covered by the provisions of this Act Relevant.
16. ***Corporate liability.*** When any of the punishable acts herein defined are knowingly committed on behalf of or for the benefit of a juridical person, by a natural person acting either individually or as part of an organ of the juridical person, who has a position's leading within, based on: (a) a power of representation of the juridical person provided the act committed falls within the scope of such authority; (b) an authority to take decisions on behalf of the juridical person provided, that the act committed falls within the scope of such authority; or (c) an authority to exercise control within the juridical person. It also includes commission of any of the punishable acts made possible due to the lack of supervision or control.

Source : PTV4 Forum on Anti-Cybercrime Law, Department of Justice Assistant Secretary Geronimo Sy

Table 2. Non-detectable cases/activities and their corresponding types of cybercrime

Non/Less Detectable Cases	Types of Cybercrime
1. Hacking **A. *IP spoofing*** (*hoax, deception, parody)* a.1 Hacker must first use a variety of techniques to find an IP address of a trusted host and then modify the packet headers so that it appears that the packets are coming from that host. a.2 they insert false or misleading information in *e-mail* or *net news* headers. Falsified headers are used to mislead the recipient, or network applications, as to the origin of a message. This is a common technique of *spammers* and *sporgers* , who wish to conceal the origin of their messages to avoid being tracked down.	1. Illegal Access 2. Illegal Interception 3. Data Interference 4. Sysyem Interference 5. Misuse of Device 6. Cyber-Squatting 7. Computer-Related Forgery 8. Computer-Related Fraud
B. *Trojan horse* This is a common mechanism for hiding viruses or worms (A virus is a code fragment that copies itself into a larger program, modifying that program. A worm is an independent program, which reproduces by copying itself in full-blown fashion from one computer to another, usually over a network). It is almost impossible to detect the presence of a Trojan horse because it does not cause any noticeable damage.	1. Data Interference 2. System Interference
2. Spam (*unsolicited e-mail*) Using *Image spam*, or Image-based spam, is an obfuscating method in which the text of the message is stored as a *GIF* or *JPEG* image and displayed in the email. This prevents text based spam filters from detecting and blocking spam messages. A newer technique, however, is to use an animated *GIF* image that does not contain clear text in its initial frame, or to contort the shapes of letters in the image (as in CAPTCHA) Completely Automated Public Turing test to tell Computers and Humans Apart") to avoid detection by OCR(optical character recognition) tools.	1. Computer-related Forgery 2. Computer-related Fraud 3. System Interference
3. Plagiarism Internet plagiarism is sometimes harder to detect than with printed materials because of the ease of which materials can be stolen. Not all documents are electronic and some are not text-based which are hard to detect. (wisegeek, n.d.).	1. Computer-related Identity Theft
4**. Pimps on line** (*flesh peddling*) 1. The use of virtual currencies and anonymous payment. 2. The use of encryption technology (ITU, 2012).	1. Cybersex 2. Child Pornography

III. RESEARCH METHODS

The study utilizes Content Analysis method to analyze cybercrime law to extract and discover if there are some cases of cybercrime that have lesser or cannot be detected. Content Analysis defined as any technique for making inferences by systematically and objectively identifying special characteristics of messages (Holshi, 1968). Analysis of data once organized according to certain content element. It evolves consideration of the literal words in the text being analyzed. In this way, Content Analysis provides a method for obtaining good access to the words of the text or transcribed accounts offered by the subject (Glassner & Loughlin, 1987). From this perspective, photographs, videotape or any item that can be made into text are amenable to Content Analysis. This gives us an opportunity to learn about how the authors of textual materials view their social world. It shows how researchers can examine ideological mind-sets, themes, topics, symbols and similar phenomena while digging such examination to the data gathered. Researchers need to examine the artifacts of social communication, typically these are written documents or transcriptions of recorded communications.

The study also utilizes the available research from government data and documentation, academic journals and books, and research engines available on line. The ultimate goal of this is to analyze the scope of cybercrime: types and cases/activities that corresponds cybercrimes that are less and cannot be detected; and what is being done about it that made it almost impossible to detect.

IV. HACKING

IP spoofing. The most dominant case of non-detectable cases and activities falls in the seven types of cybercrimes such as: (1) Illegal access; (2) Illegal interception; (3) Data interference; (4) System interference; (5) Misuse of device; (6) Computer-related forgery; (7) Computer-related fraud; and (8) Computer related forgery. It shows that Hacking is the most dominant case of non-detectable or most likely less detectable. Under the category of hacking is IP spoofing or IP address forgery and Trojan horse.

IP spoofing, also known as IP address forgery or a host file hijack, is a hijacking technique in which a cracker masquerades as a trusted host to conceal his identity, spoof a web site, hijack browsers, or gain access to a network. Here is how it works: The hijacker obtains the IP address of a legitimate host and alters packet headers so that the legitimate host appears to be the source.

When IP spoofing is used to hijack a browser, a visitor who types in the Uniform Resource Locator (URL) of a legitimate site is taken to a fraudulent web page created by the hijacker. For example, if the hijacker spoofed the Library of Congress Web site, then any internet user who typed in the URL *www.loc.gov* would see spoofed content created by the hijacker.

If a user interacts with dynamic content on a spoofed page, the hijacker can gain access to sensitive information or computer or network resources. He could steal or alter sensitive data, such as a credit card number or password, or install malware . The hijacker would also be able to take control of a compromised computer to use it as part of a zombie army in order to send out spam (Rouse, 2007).

Trojan horse. Trojans are malicious programs that perform actions that have not been authorized by the user. Unlike computer viruses and worms , Trojans are not able to self-replicate. These actions can include:

- Deleting data;
- Blocking data;
- Modifying data;
- Copying data; and
- Disrupting the performance of computers or computer networks. This is how the hacker made all the trojan and virus key logger undetectable.

1. Hackers create a server as a remote administration tool that does not have a

router.

2. They download software passport by silicon realm, since hacker consider silicon realm as the best binder to make everything 100 % undetectable by all anti viruses.
3. Once it is downloaded and installed, they will download it again for the pre-made setting and make a backup file by putting it in the same folder or location.
4. By reopening the software passport, they will click "*load existing project*" where it says "*Files to protect*" in which they will add the files they want to make non–detectable. Right after clicking the "*build project"* a bunch of windows will come up.
5. Once it is created they are 100 % undetectable. Hacker will try the code: *virustotal.com* to scan in every existing anti-virus and they will not find anything.

V. SPAM *(unsolici ted emai ls)*

Using *Image spam*, or *Image-based spam*, is an obfuscating method in which the text of the message is stored as a *GIF* or *JPEG* image and displayed in the email. This prevents text based spam filters from detecting and blocking spam messages. A newer technique, however, is to use an animated *GIF* image that does not contain clear text in its initial frame, or to contort the shapes of letters in the image (as in CAPTCHA) Completely Automated Public Turing test to tell Computers and Humans Apart") to avoid detection by OCR (optical character recognition) tools.

VI. PLAGIARISM

Plagiarism is wrongfully appropriating and stealing one's ideas and representation claiming it to be their own work or expression. Most of the time we are too open and vocal about what is in our thoughts that we wanted to express by posting it in facebook and other social network groups or sites. Because of the technology demands and the rapid change of faster access, with just one click, people might idealize and copy some works to claim it as their own in order to exercise their rights of freedom of speech and expression. In order to be undetected, they will use printed materials because of the ease of which materials can be stolen. Not all documents are electronic and some are not text-based which is hard to detect.

VII. PIMPS ON LINE (*FLESH PEDDLING*)

Child pornography. The sale of child pornography is highly profitable, with collectors willing to pay great amounts for movies and pictures depicting children in sexual context. Most material is exchanged in password–protected closed forums, which regular users and law enforcement agencies can rarely access.

There are two key factors for the exchange of child pornography acts as obstacles to the investigation of these crimes:

(1) The use of virtual currencies and anonymous payment. Cash payments enable buyers of certain goods to hide their identity, so cash is dominant in many criminal businesses. Virtual currencies may not require identification and validation, preventing law enforcement agencies from tracing money flows back to offenders.

Recently, a number of child pornography investigations have succeeded in using traces left by payments. However, where offenders make anonymous payments, it is difficult for them to be tracked. If such anonymous currencies are used by criminals, it restricts the ability of law enforcement to identify the suspects by following money transfers.

(2) The use of encryption technology. Perpetrators are increasingly encrypting their messages. Law-enforcement agencies note that offenders are using encryption technology to protect information stored on their hard disks, seriously hindering criminal investigations.

In addition to a broad criminalization of acts related to child pornography, other approaches such as the implementation of obligations on

internet services to register users or to block or filter the access to websites related to child pornography are currently under discussion.

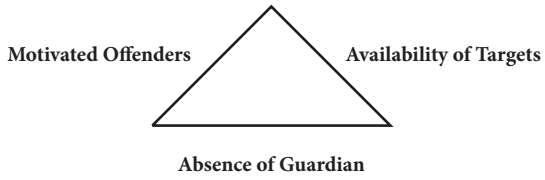
In order to prevent identification the offender had digitally modified the part of the pictures showing his face before publishing the pictures over the internet. Computer forensic experts are able to unpick the modifications and reconstruct the suspect's face. Although the successful investigation clearly demonstrates the potential of computer forensics, this case is no proof of a breakthrough in child pornography investigation. If the offender had simply covered his face with a white spot, identification would have been impossible.

One of the theoretical basis for explaining computer crime is "**Routine activities theory**." It is a criminological theory proposed by Cohen and Felson (1979).

The routine activities approach is based on two rather simple ideas:

1. It argues that in order for a crime to occur, motivated offenders must converge with suitable targets in the absence of capable guardians.
2. It argues that the probability of this occurring is influenced by our "routine activities"-including our work, family, leisure, and consumption activities.

Figure 2.1 The "Triangle of Crime" (Cohen & Felson, 1979)



Three factors/elements of this approach :

1. **The availability of suitable targets**. The technological advances produce more organizations that are dependent on computer technology, more people who have access to computers and the internet, and more computer literate individuals (Adamski, 1998). All of these factors, in turn, increase the number of suitable targets.
2. **The presence of motivated offenders.** With the increasing popularity of computer technology and hackers, more and more people have entered the hacker subculture. The exact number of hackers is unknown (Adamski, 1998). A recent study stated that the internet is an effective way for dissemination of criminal techniques, which facilitates hackers' computer crime commitment (Mann & Sutton, 1998). Consequently, the internet provides an opportunity where hacking behavior can be learned through interaction with others. Eventually, this opportunity augments the number of motivated offenders.
3. **The absence of capable guardians**. Law enforcement has not kept up with technological developments. According to the Federal Bureau of Investigation's (FBI) National Computer Crime Squad (NCCS), between 85 % and 97 % of computer intrusions are not detected (Adamski, 1998). This statistic clearly shows the current situation of law enforcement, and gives us an understanding about the magnitude of the problem.

VIII. CONCLUSION

The non-detected acts becomes a contributing factors on the increased of relative offenses concerning cybercrime. This compels a challenge for our law enforcement bodies including our criminal justice system. New schemes being created and it is very difficult to detect cybercrime cases through traditional channels. That is why cybercrime legislation must be an instantaneous concern of Congress. It is clear however, that even

with the existing Cybercrime Prevention Law in the Philippines, there still exist a need to provide a comprehensive policy framework that would set regulations on cybercrimes. There is a need for our country to have a law that will define and refine well the punishable acts involving computers with corresponding penalties, determine legal procedures for the investigation and prosecution, clarity of scope and jurisdictions, provide an effective mutual assistance and cooperation, and identify a local body that shall be responsible for providing a 24/7 assistance to foreign entities in the resolution of cybercrime cases. Agents of law enforcement should develop sophisticated technical skills which match the perpetrator's ability. Scarcity of successful detection is due mainly to the vagueness of time and space dimensions often observed in cybercrimes. Law enforcement must reinforce their equipment, communication and information infrastructure, equip law enforcement for the investigation of computer crime by providing an adequate training, providing proper equipment, allocating resources, and supplying well-defined personnel policies to strengthen their work force in order to deal these massive crises in cyber world. However, being safe and behaving properly in the internet are something we should not leave for the government to perform. This is something we can all do together.

Originality Index:	90 %
Similarity Index:	10 %
Paper ID:	470237801
Grammarly:	Checked

Adamski A. (1998). *Crimes related to the computer network. Threats and opportunities: A criminological perspective.* Helsinki, Finland: European Institute for Crime Prevention and Control, affiliated with the United Nations (HEUNI). http://www.ulapland.fi/home/oiffi/enlist/resources/HeuniWeb.htm Retrieved on 15th December 2013

Adamski, A. (1997). Legal and security aspects of information management. In Scherpenzeel, R., & Quirchmayr, G. (Eds.), *United Nations Crime and Justice Information Network: Providing Information to and from Developing Countries, A Resouce Book*. Seoul: The Hage, Vienna.

Cohen, L.E., & Felson, M. (1979). Social change and crime rate trends: A routine activity approach. *American Sociological Review*, 44(1), 588-608.

Cybercrime Prevention Act of 2012. *Republic Act No. 10175: An act defining cybercrime, providing for the prevention, investigation, suppression and the imposition of penalties therefor and for other purposes.* Retrieved from http://www.gov.ph/2012/09/12/republic-act-no-10175/

Glassner, B., & Loughlin, J., (1987). *Drugs in adolescent worlds: Burnout to straights.* New York: Palgrave Macmillan.

Holshi, O.R. (1968). Content analysis. In Lindzey, G., & Aaronson, E. (Eds.), *The handbook of social psychology*. Reading, MA: Addison-Wesley.

Lohr, S. (1997). Be paranoid: Hackers are out to get you. *New York Times Ondisk*, Access No. 13503819970317.

Mann, D., & Sutton, M. (1998). NetCrime: More change in the organisation of thieving. *The British Journal of Criminology*, 38(1), 201-229.

Peters, W.T.M. (1997, October 20). Further study in white collar crime: Hacking and criminal hacking: Computer crime. *Regulation and Control of White Collar Computer Crime.* Available: http://www.ozemail.com.au/~wtmp/wcc.html.

Rouse, M. (2007). *IP spoofing: IP address forgery or a host file hijack.* Retrieved http://searchsecurity.techtarget.com/definition/IP-spoofing

Sen, O.N. (2001). *Criminal justice responses to emerging computer crime problems*. University of Texas.