# COMBATING CYBERCRIME IN THE PHILIPPINES

*Karla T. Cabel**

## I. INTRODUCTION

On August 6, 1991, the World Wide Web (WWW) service, through the World Wide Web Project (WWW Project), made its debut to the public in the Internet. Englishman Tim Berners-Lee, the proponent of the WWW Project, envisioned that its debut would enable physicists from all over the world to conveniently share information, data, documentation and news with each other. Apparently, the public wanted to use the web for other areas and, thus, the first web message, "Collaborators welcome" of Berners-Lee, became a gateway, which allowed servers to share data on various areas of interest apart from physics.

It cannot be gainsaid that the vast majority is now enjoying the commercialization of the WWW in the 1990s. Today, the Internet has not only become a repository of information but also a tool in commerce, entertainment and social networking, both for the private sector and the government. In fact, transactions are now borderless. Credit is given to globalization, technology and the dynamic and young people of the generation.

However, the pairing of high technology and globalization results in crime in as much as borderless transactions result in borderless crimes. Today, many traditional crimes are now being committed using the computer and Internet. As correctly observed by then Federal Bureau of Investigation Director Robert Mueller, "crimes have migrated online, including various frauds, identity theft, copyright infringement, child pornography and child exploitation."[1] In one case, a teenager defrauded people of an estimated $5,000 through an on-line auction scam by advertising allegedly high-end computer equipment for sale in the Internet when, in truth, he was actually selling equipment of lesser value to unsuspecting buyers.[2]

In another case, a blogger was convicted for libel when he vented his frustration with his lawyer by calling the latter a "drug bribery mule", on his website.[3] Meanwhile, the Australian High Court allowed criminal proceedings to be held in Australia even if the servers of the article, which is the subject of the complaint, are located in New Jersey. The court ruled that the "claim could be brought only if a person had a reputation in the place where the material was published."[4]

## II. CHARACTERISTICS OF CYBERCRIME AROUND THE WORLD

### A. Types of Cybercrime and Modus Operandi

According to the Australian Institute of Criminology, there are nine (9) types of cybercrimes[5], *viz*:

1. Theft of Telecommunications Services

This occurs when offenders gain access to an organization's telephone switchboard (PBX) or dial-in/dial-out circuits, by impersonating a technician, fraudulently obtaining an employee's access code or by

*Prosecutor, Department of Justice, Padre Faura, Manila, Philippines.

[1] Targeting Cybercrime, The Philippine Star, <http://www.philstar.com/networks/184074/targeting-cybercrime> accessed February 19, 2015.

[2] Sullivan, Confessions of a Scam Artist, MSNBC, September 2002.

[3] *Milum vs. Banks*, Court of Appeals, Georgia, Case No. A06A2394, March 5, 2007.

[4] *Gutnick v Dow Jones & Co Inc*. [2001] VSC 305 (28 August 2001)', <http://www.austlii.edu.au/au/cases/vic/VSC/2001/305.html>.

[5] *9 Types of Cyber Crime*, Australian Institute of Criminology, Crime in the Digital Age by Peter Grabosky and Russell Smith, Sydney: Federation Press, 1998 (co-published with the Australian Institute of Criminology), <http://www.crime.hku.hk/cybercrime.htm> accessed February 19, 2015.

using available internet software, and use the same to make their own calls or sell call time to third parties (Gold 1999). Other forms may include "calling card details and on-selling calls charged to the calling card account, counterfeiting or unlawfully reprogramming stored value telephone cards.

2. Communications in Furtherance of Criminal Conspiracies

This involves organized criminal activities enhanced or facilitated by technology, such as weapons smuggling, money laundering, drug trafficking, gambling, prostitution and child pornography (Grant, David and Grabosky 1997).

Criminal networks have been discovered to extend transnationally, work with a significant degree of coordination and use sophisticated means of concealment. An example would be the police investigation codenamed "Operation Cathedral", which involved "Wonderland Club", an international network with 14-member nations from Europe, North America to Australia, where members can access the group and its encrypted content via password. The operation resulted to 100 arrests worldwide and seizure of over 100,000 images in September 1998.

3. Telecommunications Piracy

This involves the unauthorized reproduction of copyrighted materials for free distribution, personal use or for sale at a lower price.

Owners of the copyrighted materials are estimated to have incurred losses between $15 - $17 billion due to copyright infringement (United States, Information Infrastructure Task Force 1995, 131). The Software Publishers Association claims that it lost $7.4 billion worth of software due to piracy in 1993, of which $2 billion were stolen from the Internet (Meyer and Underwood 1994). Ryan (1998) states that American industry lost more than $10 billion in 1996, from which $1.8 billion is the estimated loss in the film industry, $1.2 billion in music, $690 million in book publishing and $3.8 billion in business application software.

4. Dissemination of Offensive Materials

This includes dissemination of objectionable materials in the Internet such as racist propaganda, sexually explicit materials and instructions for making incendiary and explosive devices, use of telecommunications systems for threatening or intrusive communications, harassing, "cyber-stalking" and other means where persistent messages are sent to unwilling recipients as well as the use of computer networks in furtherance of extortion. On June 2, 1996, the Sunday Times in England cited 4 incidents between 1993 and 1995 where senior executives of financial institutions paid £42.5 million to extortionists they believed could crash their computer systems (Denning 1999, 233-4).

In one case, a man stole nude photographs of his ex-girlfriend and new boyfriend, posting them on the Internet, along with her name, address and telephone number and maintaining records about the woman's movements and collating information about her family (Spice and Sink 1999).

A rejected suitor, using the name of the woman he courted, posted invitations on the Internet that she had fantasies of rape and gang rape, and gave out her personal information, address, phone number, her appearance and how to bypass her home security system, to which men replied and appeared at her home. Although the lady was not physically assaulted, she would not leave her home or answer the phone. She eventually lost her job (Miller 1999; Miller and Maharaj 1999).

A student in California bought information about a woman in the Internet using a professor's credit card and then sent death threats and graphic sexual descriptions to 5 female students in 1998, in response to perceived teasing about his appearance (Associated Press 1999a).

5. Electronic Money Laundering and Tax Evasion

This involves concealing and moving proceeds of crime through electronic funds transfers (money laundering) or concealing legitimately derived income from the government's taxing authorities (tax evasion) using technologies of electronic commerce.

6. Electronic Vandalism, Terrorism and Extortion

Electronic intrusion such as hacking official websites of the government or private companies, i.e. attempts to disrupt the computer systems of the Sri Lankan Government (Associated Press 1998) and North Atlantic Treaty Organization during the 1999 Belgrade Bombing (BBC 1999); German hackers who compromised an internet service provider in South Florida and demanded the delivery of $30,000 to a mail drop in Germany (Bauer 1998); and credit card details of a music retailer in North America having been obtained by an extortionist in Eastern Europe who published the details of the former on the Internet when he refused to comply with latter's demands (Markoff 2000).

7. Sales and Investment Fraud

The use of cyberspace for misinformation by directly accessing victims worldwide. This includes classic pyramiding schemes and bogus investment opportunities and investment solicitations (Cella and Stark 1997, 822).

8. Illegal Interception of Telecommunications

This involves electronic eavesdropping, such as surveillance of an unfaithful spouse, telecommunications interception and industrial espionage, by intercepting electromagnetic signals from computers. An example is the case of an American hacker, Kevin Poulsen, who accessed law enforcement and national security wiretap data (Littman 1997).

9. Electronic Funds Transfer Fraud

This involves the electronic and physical interception of valid credit card numbers and counterfeiting of digital information stored on a card.

In 1994, Russian hacker Vladimir Levin, was able to access Citibank's central wire transfer department and transferred money from large corporate accounts to the accounts of his accomplices in the United States, Finland, Germany, Netherlands and Israel. A corporate owner in Argentina notified the bank, which resulted in the arrest of his accomplices in San Francisco and Rotterdam. Levin was later arrested during a visit to the United States (Denning 1999,55).

**B. Damages Caused by Cybercrime**

Cyber-attacks have become a regular occurrence since the ubiquity of the Web. Cybercrime espionage and pilfering of personal information is believed to have affected more than 800 people during 2013. Financial losses from cyber-theft can cause as much as 150,000 European jobs.

Sometime in August 2014, there was a mass breach of privacy when about 200 images of various celebrities were posted on the image-sharing site "4chan". Most of them were intimate photos of women. The images, which were allegedly hacked from the iCloud of Apple, spread through Twitter and Reddit and other various social media sites.[6]

Still, in November 2014, a group called the "Guardians of Peace", allegedly acting in retaliation against Sony Pictures Entertainment for the release of the movie "The Interview" (a fictional story about a CIA plot to assassinate Kim Jong-un, the North Korean dictator), hacked thousands of Sony's private documents and emails. In December 2014, "Guardians of Peace" threatened cinemas with terrorist violence if the film were shown and, thus, caused several movie theaters' refusal to run it. The US Director of National Intelligence James Clapper contends that it was the North Korean General Bureau of Reconnaissance that supervised the hacking attack and that it may have caused Sony "potentially hundreds of millions of dollars in damage".[7] The attack rendered thousands of Sony computers inoperable such that the company had to take the entire network offline. Despite these assertions, experts state that there is no evidence that North Korea was behind the attack. Sony's CEO Kaz Hirai remarked that Sony was a victim of one of the most vicious and malicious cyberattacks in recent history.

---

[6] *Celebrity 4Chan Shock Naked Picture Scandal: Full List of Star Victims Preyed Upon By Hackers*, <http://www.mirror.co.uk/3am/celebrity-news/celebrity-4chan-shock-naked-picture-4395155> accessed February 19, 2015.

[7] *Sony Pictures Hack: US Intelligence Chief Says North Korea Cyberattack Was 'Most Serious' Ever Against US Interest*, <http://www.independent.co.uk/news/world/americas/us-intelligence-chief-sony-hack-was-most-serious-attack-against-us-interests-99> accessed February 19, 2015.

On December 22, 2014, a cyberattack against a German steel mill resulted to massive damage. According to the report of the German Federal Office for Information Security (BSI), the attackers used a "spear phishing" campaign aimed at particular individuals of the company to trick people into opening booby trapped emails to steal logins to access the mill's control systems. This led to failure of the plant's blast furnace to shut down normally. The unscheduled shutdown caused immense physical damage to the steel mill.[8]

More recently, on February 4, 2015, a video was aired showing Jordanian pilot Lt. Muath al-Kaseasbeh being burned alive by the Islamic State of Iraq and Syria (ISIS). The images of the killing triggered global condemnation and Jordan's promises of immediate retaliation[9]. And yet again, on February 15, 2015, ISIS released a new video showing the beheading of 21 Coptic Egyptian Christians on a Libyan beach.[10]

In 2014, reports state that the global economy is losing $445 billion annually.[11] However, recent estimates reveal that the cost of cybercrime to businesses worldwide range from $445 billion (£291 billion) to $2 trillion (£1.3 billion) a year. The cost of cybercrime will continually increase since transactions are now moving online as more companies and consumers connect to the Internet worldwide. Intellectual property theft losses will also increase because acquiring countries continually improve their abilities to manufacture competing goods.

These are but few examples of cybersecurity-related damages and cyber-sabotage, which terrorists and/or hostile elements could mount. Indubitably, cybercrime is becoming more pervasive through the years. Measures to secure cyberspace will be fraught with challenges since the Internet was designed to promote connectivity and not security. Still, governments should come up with effective ways to collect and publish cybercrime-related data to enable its people to make better choices on Web-related risks and policies.

## III. THE CYBERCRIME PREVENTION ACT OF 2012 OF THE PHILIPPINES

In reply to the challenges of cybercrime, the Philippines enacted its first law regulating the WWW on June 14, 2000, Republic Act No. 8792 (Philippine Electronic Commerce Act of 2000). This was done after a criminal complaint, which was filed against the suspected creator of the email Trojan called "ILOVEYOU", was dismissed due to then absence of concrete laws regulating the Web in the Philippines.

On September 12, 2012, Republic Act No. 10175 (The Cybercrime Prevention Act of 2012) was signed into law. However, the law became effective only after the Supreme Court of the Philippines upheld the validity of its salient parts in its Decision dated February 18, 2014.[12]

## IV. THE INVESTIGATION, PROSECUTION AND ADJUDICATION OF CYBERCRIME

### A. Initial Information Gathering

1. Cyberpatrol

The Cybercrime Division of the National Bureau of Investigation (NBI) and the Anti-Cybercrime Group of the Philippine National Police (PNP) are the law enforcement agencies (LEA) responsible for the investigation and prevention of cybercrime in the Philippines. They are also required, under the law, to submit regular reports, including pre-operation, post-operation and investigation results and other documents,

---

[8] *Hack Attack Causes 'Massive Damage at Steel Works*, BBC News, December 22, 2014 <http://www.bbc.com/news/technology-30575104> accessed February 19, 2015.

[9] *Fox News Airs Images of Burning Jordanian Pilot*, Huffpost Media, February 4, 2015, <http://www.huffingtonpost.com/2015/02/04/fox-news-burning-isis-hostage-jordanian-pilot-images-pictures_n_6612446.html> accessed February 19, 2015.

[10] *ISIS Posts Video of Purported Mass Beheading*, CNN International Edition, February 15, 2015 <http://edition.cnn.com/videos/world/2015/02/15/isis-video-purports-21-coptic-christian-hostages-beheaded.cnn> accessed February 19, 2015.

[11] *Cybercrime Costs Global Economy $445 BN Annually*, Rhiannon Williams, June 9, 2014, <http://www.telegraph.co.uk/technology/internet-security/10886640/Cyber-crime-costs-global-economy-445-bn-annually.html> accessed February 19, 2015.

[12] *Disini, et. al. vs. The Secretary of Justice, et. al.* GR Nos. 203335, 203299, 203306, 203359, 203378, 203391, 203407, 203440, 203453, 203454, 203469, 203501, 203509, 203515, 203518, February 18, 2014.

which may be required by the Department of Justice – Office of Cybercrime (DOJ-OOC) for review and monitoring.[13]

2. Reporting System

The Department of Justice of Justice – Office of Cybercrime (DOJ-OOC) is the central authority in the monitoring of all matters relating to cybercrime. Its functions also include receiving regular reports from the LEA.[14]

**B. Tracing and Identifying Criminals, Preserving and Collecting Evidence**

1. Tracing and Identifying by IP Address and other Measures

The first step in prosecuting cybercrime cases is for the responsible LEA to identify who the criminal is by determining his/her Internet Protocol Address (IP Address)[15]. The challenge online is that there are innumerable measures to hide one's identity, such as the use of services that will mask a user's IP Address by routing traffic through various servers.

However, diligence pays in tracking down cybercriminals. It has been observed in several cases that those who engage in cyber-stalking or cyber-fraud, to name a few, are not technically savvy and may leave clues as to their identity within the content of the data. It has been further observed that even experts may inadvertently leave clues due to their complacency or sheer arrogance.

Ordinarily, IP Address can be extracted through the header information of emails and system logs. Once the IP Address has been identified, the said IP Address is then subjected to a WHOIS search, a query and response protocol that is widely used for querying databases that store the registered users or assignees of an internet resource[16], to verify which Internet Service Provider (ISP)[17] it belongs to. Examples of WHOIS lookup capable websites are "www.Checkdomain.com" and "www.apnic.net".

When the ISP is identified, a Preservation Order is then sent to the ISP requiring it to preserve the integrity and content of the data in their custody for a minimum period of six (6) months from the date of receipt of the said order[18]. The law provides that the Service Provider shall keep confidential the order and its compliance.

2. Real-Time Collection of Traffic Data and Interception of Content Data

It is recommended that the LEA conduct a thorough investigation before executing a search warrant of the scene of computer-related crime to avoid delays since they will know in advance what to expect at the crime scene and will be able to determine whether there is a need for experts for purposes of collecting data.

The LEA may conduct either technical surveillance or physical surveillance in their investigation. Technical surveillance, if applicable, is done by visiting the website concerned with the intention of downloading resource materials therefrom and establishing communication with the subject through email. On the other hand, physical surveillance entails verifying the existence of the addresses provided by the ISP by going to the indicated address and comparing the results to the information received.

3. Fair and Timely Search, Seizure and Preservation of Digital Evidence

Using the resource materials and valuable information obtained from the surveillance, the LEA will then secure a search warrant from the court. Thereafter, pursuant to the said warrant, it shall order the ISP to disclose or submit the subscriber's information, traffic data or relevant data in its possession or control within seventy-two (72) hours.[19]

---

[13] Sec. 11, Ibid.
[14] Sec. 23, Ibid.
[15] IP Address – series of numbers assigned by an Internet Service Provider to an internet user when it connects to the Internet. Anchor of all crimes committed via Internet.
[16] <En.wikipedia.org/wiki/Whois> accessed February 20, 2015.
[17] Internet Service Provider – provides internet service to internet users.
[18] Sec. 13, Republic Act No. 10175.
[19] Ibid.

It is recommended that the execution of the warrant be documented either through writing, sketching, photographs and/or video. Situational awareness is paramount. Thus, it is crucial to always secure and take control of the scene bearing in mind the team's safety. As soon as the area has been secured, the forensic investigator may now run the incident response (IR) tools and save volatile data. The LEA should not access computer files in the search area. If the computer is off, it should be left off. If it is on, they should refrain from searching the computer. Instead, photograph the screen, if something is displayed on the monitor, and consult with the on-site forensic investigator.

When executing the search warrant, the LEA should keep individuals, especially the suspect, away from computer equipment to avoid corruption of the data. However, if the computer appears to be destroying the evidence, they should immediately shut it down by pulling the power cord.

The LEA should secure the seized evidence by properly bagging[20] and tagging[21] them and placing them in non-magnetic containers to be examined by a certified forensic media analyst. The LEA should properly transport electronic evidence obtained from the crime scene. The computer evidence should not be exposed to heat and radio transmission. Radio transmitters can damage the hard drive and destroy the evidence. Meanwhile, the evidence should be stored in an area inaccessible to unauthorized persons. Cool and dry storage facilities away from generators and magnets are ideal.

4. Technical Analysis of Digital Data

Evidence should be evaluated with the assistance of experts on digital forensics[22]. This is because computer evidence require knowledge in a wide array of programming systems, such as d-base III, Lotus 1-2-3 and other word processing languages, which are not known even to the best trained investigators. Since digital evidence can be easily altered, its analysis should be done by experts to preserve its integrity and authenticity. Digital forensics determines the cause of the cybercrime, the manner in which it was committed, leads on the cybercriminal and existence of contraband by analyzing not only digital data but also its relation to the pieces of documentary evidence recovered from the area of search.

**C. Prosecution**

1. Appropriate Evaluation of Digital Evidence

Although digital evidence is accorded evidentiary value as other forms of evidence, i.e. object, documentary, testimonial, there is always hesitation in presenting them in court. This is attributed to the complexity of digital evidence, lack of technical know-how of both the bench and bar and improper collection of digital evidence. But what makes digital evidence the least favorite among other forms of evidence is that it is "extremely vulnerable to inadvertent or intentional modification or destruction".[23]

A simple misstep in the collection of digital evidence can affect the integrity of the data content. Improper handling and storage of digital evidence can easily corrupt it, and evidence haphazardly gathered by untrained investigators may be excluded by the court for incompetence.

*Apropos*, digital evidence should be properly evaluated before it is presented in court.

To avert issues on the integrity and authenticity of digital evidence, it is recommended that LEA apply for search warrants when seizing digital evidence.[24] This will ensure that the evidence is properly documented, gathered, identified, examined and preserved.

In drafting the affidavit application of the warrant, the LEA will indicate therein the facts established through an Internet Protocol (IP) Address, subscriber account, or mobile phone number, call logs for a specific period or duration, describe with particularity the data or information to be disclosed and the

[20] Bagging – protects against contamination and tampering.
[21] Tagging – provides means of associating the attached and bagged evidence with a particular date, time, location, place event and seizing agent.
[22] Digital Forensics – refers to the application of investigative and analytical techniques that conform to evidentiary standards used in or appropriate for a court of law of other legal context.
[23] McCullagh, *Electronic Evidence Anchors Porn Case*, Tech News CNET.com, August 29, 2002.
[24] Manual of Guidelines in Investigating Cybercrimes.

specific violation of the law.[25]

In the recent landmark case of *Riley vs. California*, the 4th Appellate District, Division One of California, ruled that warrantless police searches of the contents of an arrestees' cell phones is not allowed. It opined that cellphones are tiny computers with highly private data and accessing them is different from going through someone's pockets or purse.[26]

Note, however, that in *Warshak vs. United States of America*[27], the Sixth US Circuit Court of Appeals proscribed investigators from conducting email searches in a fraud case filed against an individual ruling that e-mail users maintain a "reasonable expectation of privacy in the content of their emails". It held that although a third party has access to email, like an internet service provider, this does not mean that a subpoena can compel the said provider to defeat the accused's privacy by opening the latter's emails and presenting them to the investigators.[28]

As regards the evaluation of digital documents, such as computer print-outs and e-mails, the law provides that they are considered admissible provided they comply with rules of admissibility under the Rules and that they are properly authenticated.[29] Further, electronic documents are authenticated by evidence showing that they have been digitally signed by the person purported to have signed the same, evidence that appropriate security procedures or devices for authentication of electronic evidence were applied and by evidence showing its integrity and reliability to the satisfaction of the judge.[30] In one case, the Supreme Court ruled that the computer print-outs which were submitted in evidence were unauthenticated, unreliable and, thus, found them insufficient to establish the allegations of absenteeism and tardiness.[31]

It is also necessary that the chain of custody of digital evidence is observed when evaluating the said evidence. It is always the burden of the prosecution to convince the court that the digital evidence being offered has not been modified or replicated. Thus, any change in the chain of custody must be properly documented. Otherwise, the evidence may not be presented at a later date or be discarded by the court for lack of authenticity and integrity.

2. Identifying Criminal Acts and Proper Selection of Cybercrime Charges

Republic Act No. 10175 enumerates and defines cybercrime offences. According to the said law, punishable offences are as follows: (i) those offences against the confidentiality, integrity and availability of computer data and systems, *viz*: illegal access[32], illegal interception[33], data interference[34], system interference[35], misuse of devices[36] and cybersquatting[37]; (ii) computer-related offences, *viz*: computer-related forgery[38], computer-related fraud[39], computer-related identity theft[40]; (iii) content-related offences, *viz*: cybersex[41], child pornography[42] and libel[43] (iv) other cybercrimes, *viz*: aiding, abetting and attempting to commit punishable acts enumerated under the said law and (v) crimes committed under the Revised Penal Code and Special Laws, if committed by, through and with the use of information technology.

Apart from being charged for violation of Republic Act No. 10175, the offender may also be charged for

---

[25] Section 4, Republic Act No. 10175.
[26] *Riley vs. California*, Case No. 13-132, June 25n, 2014.
[27] *Warshak vs. US*, Case No. 06-4092, June 18, 2007.
[28] *Warshak vs. US*, supra.
[29] Section 2, Rules on Electronic Evidence.
[30] Section 2, Rule 5, Ibid.
[31] *Asuncion vs. National Labor Relations Commission, et. al.*, G.R. No. 129329, July 31 2001.
[32] Illegal Access – the access to the whole or any part of computer system without right (Sec.4 par.a[1], R.A. No. 10175.
[33] Illegal Interception – the interception made by technical means without right of any non-public transmission of computer date to, from a computer system carrying such computer data (Sec. 4, par.a[2], Ibid).
[34] Data Interference – intentional or reckless alteration, damaging, deletion or deterioration of computer data, electronic document, or electronic data message, without right, including the introduction or transmission of viruses (Sec.4, par.a[3], Ibid).
[35] System Interference – intentional alteration or reckless hindering or interference with the functioning of a computer or computer network by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data or program, electronic document, or electronic data message, without right or authority, including the introduction or transmission of viruses (Sec.4, par.a[4], Ibid).
[36] (Sec.4, par.a[5], Ibid).

violating other related laws, such as Special Protection of Children Against Child Abuse, Exploitation and Discrimination (Republic Act No. 7610), as amended; Terrorism Financing Prevention and Suppression Act of 2012 (Republic Act No. 10168); Electronic Commerce Act (Republic Act No. 8792); Anti-Money Laundering Act 2001 (Republic Act No. 9160, as amended by R.A. 9194); Comprehensive Dangerous Drugs Act of 2002 (Republic Act No. 9165); Anti-Trafficking in Persons Act of 2003 (Republic Act No. 9208, as amended by Republic Act No. 10364); Anti-Photo and Voyeurism Act of 2009 (Republic Act No. 9995); Anti-Child Pornography Act of 2009 (Republic Act No.9775), E-Commerce Act of 2000 (Republic Act No. 8792); Access Device Regulation Act of 1998 (Republic Act No. 8484); Intellectual Property Code of the Philippines (Republic Act No. 8293) and for other common crimes under the Revised Penal Code of the Philippines.

## V. CAPACITY BUILDING

Ill-equipped and ill-trained investigators in the field of cybercrime are anathema to the successful prosecution of cybercrime offences, not only in the Philippines, but worldwide. It is predicted that cybercrime will treble over the next three (3) years and yet the personnel in the Philippines involved in cybercrime are not prepared to deal with cyber-threats.

In November 2014, a group identified as "BloodSec International", defaced websites of the bills payment center Expresspay, the government's Technical Education and Skills Development-Calabarzon and the Philippine Society of Nephrology after attacking Globe Telecom's website.[44]

Still in November 2014, a group identified as "Anonymous Philippines" hacked 38 government websites posting a message calling Filipinos to join a protest against corruption.[45] In January 2015, various government websites were hacked again by Anonymous Philippines calling for justice for the 44 slain policemen of the Special Action Force of the Philippine National Police.[46]

To address this issue of readiness, from November 24-28, 2014, the OOC, in partnership with the Council of Europe (COE) and European Union (EU), conducted a Judicial and Law Enforcement Training Workshop on Cybercrime. The workshop integrated the tasks of the OOC in line with the COE EU Global Action against Cybercrime (GLACY) project. The training was attended by judges and law enforcers who are handling electronic evidence.

In February 2014, the OOC conducted the second phase of the Basic Cybercrime Ethical Hacking

---

[37] Cybersquatting – acquisition of domain name over the internet in bad faith to profit, mislead, destroy reputation and deprive others from registering the same.
[38] Computer-related forgery – input, alteration or deletion of computer data without right 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 directly readable and intelligible or the act of knowingly using computer data which is the product of computer-related forgery as defined herein, for the purpose of perpetrating a fraudulent or dishonest design.
[39] Computer-related fraud – the unauthorized input, alteration or deletion of computer data or program or interference in the functioning of a computer system, causing damage thereby with fraudulent intent: Provided, that if no damage has yet been caused, the penalty imposable shall be one (1) degree lower.
[40] Computer-related identity theft – intentional acquisition, use, misuse, transfer, possession, alteration or deletion of identifying information belonging to another, whether natural or juridical, without right: Provided, that if no damage has yet been caused, the penalty impossible shall be one (1) degree lower.
[41] 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.
[42] Child-pornography- unlawful or prohibited acts defined and punishable by Republic Act No. 9775, committed through a computer system: provided, that the penalty to be imposed shall be one (1) degree higher.
[43] 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 which may be devised in the future.
[44] After Globe, More PH Websites Hacked, inquirer.net, <technology.inquirer.net/39602/after-globe-more-ph-websites-hacked> accessed February 21, 2015.
[45] *Antipork Hackers Hit 38 Government Websites*, <technology.inquirer.net/31145/antipork-hackers-hit-38-govt-website> accessed February 21, 2015.
[46] *Hackers Attack Government Sites, Call For Justice for Slain SAF Men, Nestor Corrales*, Inquirer.net, <technology.inquirer.net/40558/hackers-attack-govt-sites-call-for-justice-for-slain-saf-men> accessed February 21, 2015.

Training of law enforcers. This was graced by the operatives from the National Bureau of Investigation-Cybercrime Division (NBI-CCD) and the Philippine National Police-Anti-Cybercrime Group (PNP-ACG).

Since digital forensics in cyber-related offences is a complex subject, training programmes are not only given to law enforcers but also to prosecutors, state counsels and public attorneys in the Philippines. The coverage of the training includes procedures on cybercrime investigations, cyber-incident response and digital forensics.

The OOC will also launch the National Computer Forensics Training Program, a consolidated training for all law enforcers in computer forensics and provide them with structured procedures and guidelines consistent with international best practices.

Another challenge in cybercrime is interstate coordination. Rising incidents of cybercrime show that it is a global phenomenon where a cybercriminal stationed in one state executes his attacks in another unsuspecting state.

Thus, in January 2014, the OOC started formulating the Global Action on Cybercrime (GLACY) project country report and work plan. This is in partnership with the Council of Europe (COE). This project aims to enable criminal justice authorities to engage in international cooperation on cybercrime and electronic evidence on the basis of the Budapest Convention.

The OOC has also been coordinating with the United States Homeland Security Investigations (USHSI) Manila Attaché in the investigation of crimes, such as child pornography, with the use of the Internet. The coordination led to a successful operation and arrest of a subject in contact with an American sex predator in the United States sometime in February 2014.

Considering that combating child pornography is a priority of the OCC, the OOC is developing a centralized "flat file" database of child pornography collated from investigations and intelligence gathering. The database will be disseminated to all ISPs to serve as a reference for "filtering and blocking". The project is in collaboration with the International Police's International Child Sexual Exploitation (INTERPOL ICSE). INTERPOL will conduct training in the ICSE in April 2015.

## VI. CONCLUSION

The growth of cybercrime is alarming. Recent surveys show that with advancements in technology and anonymity in the Internet, cybercrime will increase in severity and in number over the years. Be that as it may, cybercrime is a threat to all sectors of society worldwide. Private business entities such as banks, infrastructure, software companies, copyrighted materials and government offices are not spared from cyber-threats. A cybercriminal stationed in one country can commit a crime in another state with impunity.

Jurisdiction in cybercrime becomes a real issue especially when the perpetrator hides behind the veil of a country with unregulated cyber-activities. In this regard, the principle of sovereignty, which dictates that a law of one country cannot be imposed upon anther, becomes a bane to cybercrime prosecution. Crime is borderless but the enforcers are restricted by the borders of sovereignty.

With this realization, more and more countries are now adopting an inter-country cooperation approach against cybercrime. Inter-state treaties harmonize laws in signatory countries and establish systems of mutual cooperation.

Although some object to the "seeming" interference of foreign states on one's territory, the same is a small price to pay compared to the magnitude of damages and terror the cybercriminals can cause if they are allowed unabated access to the Internet.