COUNTRY REPORT ON CYBERCRIME: THE PHILIPPINES

*Gilbert C. Sosa**

I. INTRODUCTION

Cybercrime goes beyond the technical, transnational dimension and involves offenders who deliberately fashion their attacks to exploit the potential weaknesses present in the infrastructure's transnational nature. It threatens the substantial and growing reliance of commerce, governments, and the public upon the information infrastructure to conduct business, carry messages, and process information.

Cybercrime is one of the fastest growing non-violent crimes in the Asian region. It takes a great deal of technical expertise and co-operation, both local and foreign, in order to address such problems. This crime affects different countries in varying degrees, depending on the extent of the legislative enactment of each country. In the Philippines, as technical and electronic landscapes change, there is a need to enact laws or amend existing laws to fully address cyber threats.

II. PHILIPPINE SITUATION

A. Government Responses

The public is aware of the importance of legislation that supports police efforts against computer crimes. Onel de Guzman, the Philippine dropout who, in August 2000, created and unleashed a remarkably dangerous computer virus called "I LOVE YOU", cost several companies, governments, and citizens billions of US dollars in damages. In August of the same year, charges against him in our country were dismissed, mainly because we had not yet passed legislation addressing the crimes he had committed. The public around the world is justifiably outraged.

1. The "I LOVE YOU" Computer Virus

The virus was received in e-mail inboxes in Hong Kong on 4 May, 2000, with subject "I LOVE YOU" and an attachment "LOVE-LETTER-FOR-YOU.TXT.vbs.". It erases or blurs the graphics and data in the computer and gets the contact addresses in the computer directory, and sends the same email to all contacts listed in that directory. Once received and opened in another computer, it replicates all that it did previously. The replication went on and on, sweeping all computers where the email was received and opened, from Hong Kong, to Europe, to the United States, infecting and damaging computers and networks of small and big companies, private and government institutions. The damage was about US$ 5.5 billion; some reports say US$ 10 billion.

2. Arrest of the Suspect

An international manhunt was conducted; the investigators traced the origin of the virus to its creator, a programming student (Onel de Guzman) at the AMA Computer University in Manila.

When arrested (11 May 2000), the suspect apologized to the public and said he had no intention of causing such great harm. Government prosecutors filed cases against him, but even at the first stage, the indictment was dismissed as there was no law penalizing the act at the time (May 2000) in the Philippines (*nullum crimen, sine lege*)!

3. Effect of the "I LOVE YOU" Virus

The "I LOVE YOU" virus illustrated that a person armed with a computer could, from a distant location, attack and/or disrupt computers and networks worldwide and cause severe damage.

---

* Chief, Anti-Transnational Crime Division of Criminal Investigation and Detection Group, Philippine National Police.

This whole episode points to the need for a domestic law to address a particular criminal act, and international/bilateral legal instruments to give "no-safe haven" to cyber-criminals (or would-be cyber-terrorists).

The Philippine Congress subsequently passed a law that penalizes computer/cybercrimes, although it did not cover cyber-terrorism.

4. Congress' Response

In order to curb the threat posed by cybercrime, the Philippine Congress enacted Republic Act (RA) 8792, otherwise known as the "Electronic Commerce Act of 2000". RA 8792 provides for the legal recognition and admissibility of electronic data messages, documents and signatures. This was signed into law on 14 June 2000. The salient features of the Act are as follows:

- Provides for the admissibility of electronic documents in court cases;
- Penalizes limited online crime, such as hacking, introduction of viruses and copyright violations of at least Php100,000 and a maximum commensurate to the damage incurred, and imprisonment of six months to three years, among others;
- Promotes e-commerce in the country, particularly in business-to-business and business-to-consumer transactions whereby business relations are enhanced and facilitated and consumers are able to find and purchase products online;
- Aims to reduce graft and corruption in government as it lessens personal interaction between government agents and private individuals.

RA 8792 is considered the landmark law in the history of the Philippines as a legitimate player in the global marketplace. It has placed the Philippines among the countries penalizing cybercrime.

Likewise, the Supreme Court drafted the Rules on Electronic Evidence, which took effect on 1 August 2000, to emphasize the admissibility of evidence in electronic form, subject to its authenticity and reliability. This restriction intends to safeguard against accepting evidence of doubtful character.

We have also the Access Devices Regulation Act of 1998 (RA 8484) which regulates the issuance and use of access devices, prohibiting fraudulent acts committed and providing penalties and for other purposes; and, Philippine Central Bank Circular 240 dated 7 April 2000 regulating the electronic banking services of financial institutions.

While RA 8792 is already in place, it was found to have failed to address all forms of cybercrime that are enumerated in the Budapest Convention on Cybercrime of 2001, namely:

- Offences against confidentiality, integrity and availability of computer data and systems which include illegal access, illegal interception, data interference, system interference, misuse of devices;
- Computer-related offences which include computer-related forgery and computer-related fraud;
- Content-related offences such as child pornography;
- Offences related to infringement of copyright and related rights.

Furthermore, enforcing the law with the use of the existing guidelines embodied in the Revised Penal Code, as amended, may not work for cybercrime. Unlike the traditional and terrestrial crimes which deal with corporeal evidence, cybercrime involves more electronic data which are intangible evidence.

In order to cope with the daunting problem of cybercrime, the Department of Justice (DOJ) created the Task Force on E-Government, Cyber-security and Cybercrime in 2007 to deal with cyber-security issues in relation to legislation and investigation. It was created to pursue the e-government agenda, institutionalize a cyber-security regime and implement laws. The said task force worked closely with the Council of Europe, a private organization, and local experts composed of IT practitioners and other stakeholders.

Among the top priorities of the Task Force was to work for the passage of the cybercrime prevention act, and the Task Force proposes the creation of e-courts to oversee all high-tech cases of hacking or crimes committed using Internet technology. Included in its effort is capacity-building of the technical knowledge of government prosecutors and judges whose courtrooms will be designated e-courts.

A related Technical Working Group (TWG) on Cybercrime and Cyber-security consists of representatives from National Government Agencies, including law enforcement agencies like the Philippine National Police (PNP), National Bureau of Investigation (NBI), private companies and academia, which have joined hands in order to address issues relating to cyber-security and cybercrime in the Philippines. It aims to consolidate and make concrete the government's efforts on cyber-security and to successfully implement measures to fight cybercrime.

The TWG drafted and proposed a bill that will supplement the current RA 8792. The proposed cybercrime bill includes a definition of cybercrime, penalties and provisions on Internet piracy and provisions on co-operation with the international community.

The proposed bill covers not only computers and computer networks but mobile devices as well. The bill will also have anti-spam measures, and will cover SMS or text messaging for mobile phones, treating mobile phones as "communication devices".

Another added provision concerns "corporate liability" and proposes that a company can be held liable for cybercrimes like hacking or virus attacks when its computer network is utilized in the commission of prohibited acts.

The bill also proposes to create a Computer Emergency Response Council (CERC) under the supervision and control of the Office of the President to formulate and implement a national action plan to address and combat cybercrime. The CERC shall be headed by the Chairman of the Commission on Information and Communications Technology (CICT). Other members shall be the Director of the National Bureau of Investigation (NBI) as Vice Chairman and Director General of the Philippine National Police (PNP), the Head of the National Prosecution Service (NPS), the Head of the National Computer Center (NCC), the Head of the Philippine Center on Transnational Crime (PCTC), the Head of the Anti-Fraud and Computer Crimes Division (AFCCD) of the NBI and the Head of the Criminal Investigation and Detection Group (CIDG) of the PNP, as well as three representatives from the private sector involved in information security, to be appointed by the President as members.

On 26 September 2007, the Philippines signed the United Nations Convention on the Use of Electronic Communications in International Contracts at United Nations Headquarters in New York. Adopted by the United Nations General Assembly on 23 November 2005, the United Nations Convention on the Use of Electronic Communications in International Contracts aims to enhance legal certainty and commercial predictability where electronic communications are used in relation to international contracts.

In October 2007, the "Legislators and Experts Workshop on Cybercrime", led by the Commission on Information and Communications Technology (CICT), declared their support for Philippine accession to the Budapest Convention on Cybercrime and the expeditious passage of an implementing anti-cybercrime law to prevent, mitigate, and deter the commission of ICT related crimes, to foster co-operation within the ICT community, government, private sector and civil society in promoting an atmosphere of safe computing.

The United Nations Commission on International Trade Law (UNCITRAL) is the core legal body of the United Nations system in the field of international trade law. Its mandate is to remove legal obstacles to international trade by progressively modernizing and harmonizing trade law. It prepares legal texts in a number of key areas such as international commercial dispute settlement, electronic commerce, insolvency, international payments, sale of goods, transport law, procurement and infrastructure development. UNCITRAL also provides technical assistance to law reform activities, including assisting member states to review and assess their law reform needs and to draft the legislation required to implement law.

B. The Philippine National Police (PNP) Efforts

At the forefront of this cybercrime information campaign is the Anti-Transnational Crime Division (ATCD) of the Criminal Investigation and Detection Group (CIDG) of the Philippine National Police (PNP).

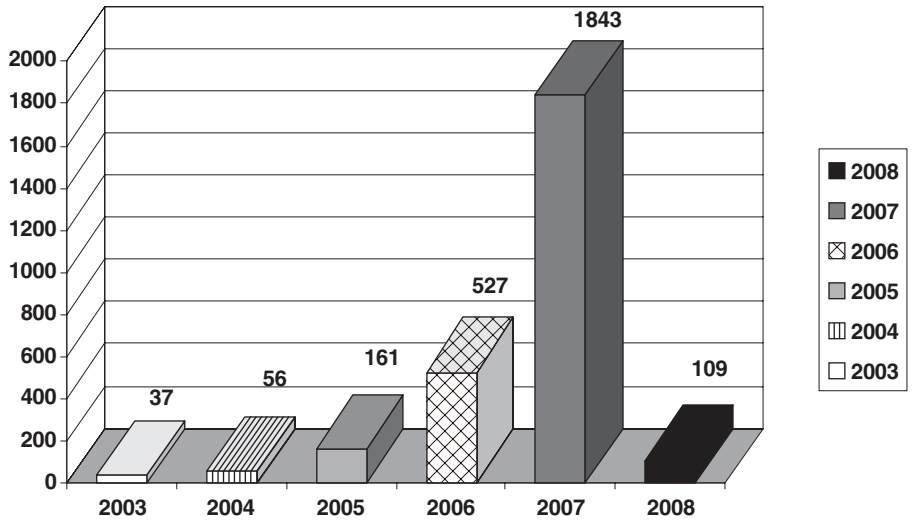
The ATCD-CIDG has a dedicated computer forensic laboratory manned by certified computer forensic examiners (EnCE) and trained computer crime investigators.

At present, numerous reports of emerging cybercrimes are emanating from the country, particularly cyber-sex and child trafficking rings.

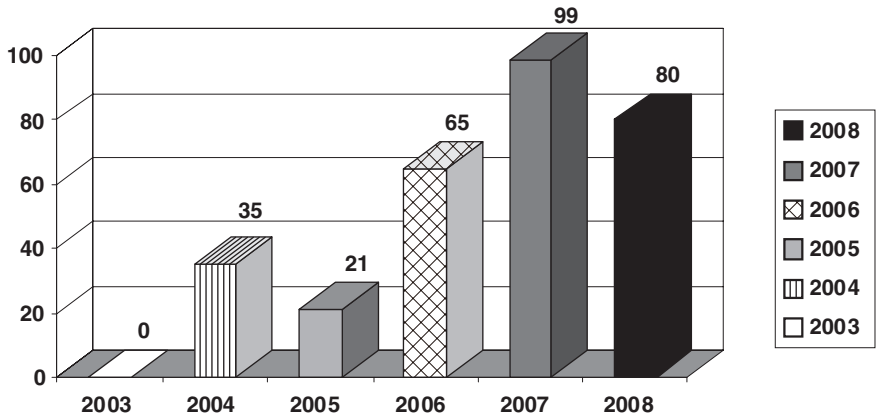
With this development, the PNP has focused its efforts on a cybercrime information campaign within the organization. It aims to promote a deeper understanding of the impact of cybercrime and to solicit the concerns and insights of the community on cybercrime-related incidents. Likewise, it has also established links with foreign counterparts in order to successfully fight the threat posed by cybercrime operations.

The first Filipino to be convicted of cybercrime, particularly hacking, was JJ Maria Giner. He was convicted in September 2005 by Manila MTC Branch 14 Judge Rosalyn Mislos-Loja. Giner pleaded guilty to hacking the government portal "gov.ph" and other government websites. He was sentenced to one to two years of imprisonment and fined Php100,000. However, he immediately applied for probation, which was eventually granted by the court. The conviction is now considered a landmark case, as he is the first local hacker to be convicted under section 33a of the E-Commerce Law or Republic Act 8792.

The Anti-Transnational Crime Division (ATCD) of the Criminal Investigation and Detection Group of the Philippine National Police (PNP-CIDG) was involved in the gathering of electronic evidence and the tracking down of the Filipino hacker with help from local Internet service provider Bitstop Inc., which hosted the gov.ph portal when it was attacked by Giner.



Computer Crime Case
2003 – July 2008

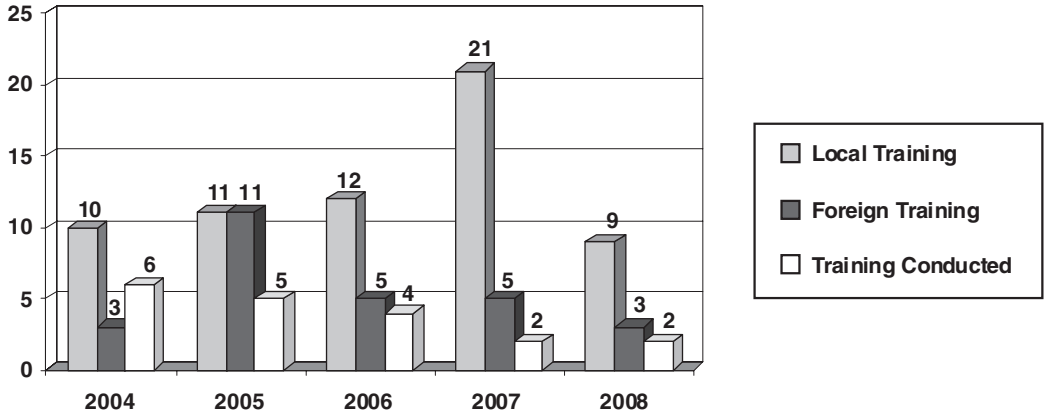


Forensic Examination
2003 – July 2008

Since its creation as a Division of the CIDG in 2003, the ATCD has encountered 2,624 referred cases of computer crimes both from government agencies and private individuals nationwide. Likewise, from CY 2004 to CY 2007, a total of 195 computer forensic examinations were also conducted.

At present, based on records from the DOJ Task Force on E-Government, Cyber-security and Cybercrimes, more than 30 cybercrime cases were filed before Philippine courts on cases relating to website defacements, on-line pornography cyber-stalking, Internet libel, computer forgery, text scams, and privacy issues.

In order to beef-up its capabilities to handle various computer-related endeavours, the ATCD-CIDG personnel received a total of 67 training sessions, both local and abroad, from 2003 to 2008. Likewise, a total of 13 training sessions were conducted for 426 personnel of the PNP nationwide.



Training Attended and Conducted by ATCD Personnel
2004 – July 2008

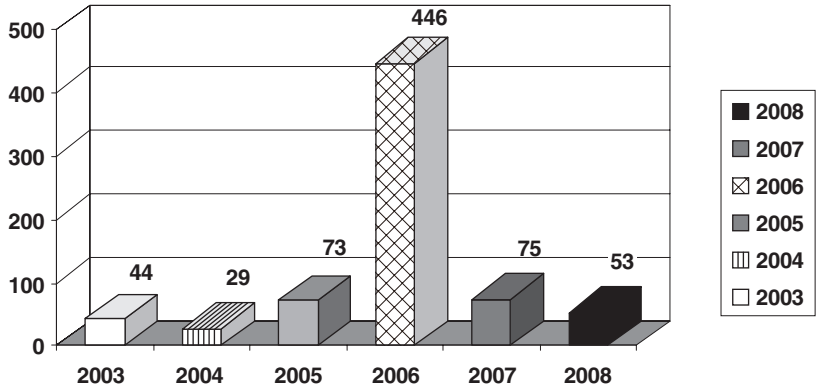
C. Philippine Emergency Response Team (PHCERT)

The first computer emergency response team or CERT in the Philippines is the PH-CERT. PH-CERT provides assistance or responses to cyber incidents locally. PH-CERT funding has to come from its membership fees and sponsorships, thus it cannot afford to have permanent staff and its services are purely voluntary. Its Concept of Operation of providing assistance is email-based and phone-based and on-site services are very minimal or do not exist. The organization has a strong co-ordination with law enforcement agencies through the conduct of technical training. However, lately, the operation of PH-CERT encountered difficulty due to lack of financial support and human resources.

D. Government Computer Security and Incident Response Team (GCSIRT)

GCSIRT was created through the Task Force on Security of Critical Infrastructure (TFSCI) and its aim is to suppress, detect and investigate computer network intrusions and other related Internet or computer crimes.

In research conducted by the GCSIRT from CY 2003 to CY 2007, there was evidence of transnational attacks on computers and the information infrastructure and a total of 667 government websites were discovered defaced, or an aggregate of 133 government websites were attacked by defacers/hackers each year, an average of 11 incidents per month. Based on this research, it was found out that 134 coded defacers (both local and international) have attacked these government websites in that five-year period. Of the attacked/hacked government websites, 507 of the 667 government websites were using the Linux operating system (OS), free and openly available software. This operating system (OS) is the most prone to attacks by defacers/hackers.



Government Web Site Defacements
(2003 -2008)

III. ISSUES

Despite the overwhelming efforts of the government and the private sector in combating cybercrime in the Philippines still much has yet to be done. The following issues hamper the effective security and protection of Philippine cyberspace:

A. Legislation against Cybercrime

The present laws are not sufficient to completely deter cyber-offenders and to protect the Philippines' cyberspace. For instance, the most important cyber-security legislation in the country, which is Republic Act 8792 or the E-Commerce Act, enacted on 14 June 2000, only penalizes hacking, cracking and piracy. It does not provide penalties for other cybercrimes such as cyber-fraud and similar offences.

B. Budgetary Constraints

Though Government spending in ICT is rising, the amount intended for the security of ICT and cybercrime prevention is very minimal.

C. Overlapping Roles of IT Government Bodies

There is no single overall government body that is mandated to address the problem of cybercrimes and to institute policies on combating such. The proliferation of different ICT committees and task forces in the government yields multiple and murky ICT directions.

D. Lack of Information Sharing, Co-ordination and Co-operation among the Stakeholders

Although there have been conferences and multilateral co-operation undertaken by the government and the private sector to develop information sharing and intelligence, still there is no established contact point for co-operation and co-ordination.

E. Lack of Proper Training of Law Enforcers

Most law enforcers do not have the proper training on computer forensics, investigation and handling of digital evidence. Worse, some do not have basic understanding of the concepts of cyber-security and cybercrime.

F. Public Awareness

Up to this time, the general public is not yet properly educated on the debilitating effect of cyber intrusions and improper computer ethics. The public should understand its role in securing the country's cyberspace.

IV. CONCLUSION

The challenge of controlling transnational cybercrime requires a full range of responses, including both voluntary and legally mandated co-operation. The government must actively pursue transnational initiatives, either voluntary, informal exchange of information, or multilateral treaties to establish a common and substantial degree of co-operation in the investigation and prosecution of cybercrime offences, since at present, there are widespread disparities among states, in the legal, regulatory, or policy environment concerning cybercrime.

With all the consolidation, revisions and filing anew of the improved version of the bills and trying to align these with the Budapest treaty, Congress has yet to act on the pending bills aimed at enacting cybercrime law in the Philippines.

Prosecutors and judges must possess technical know-how in litigating cybercrime cases.

The law enforcement agencies need specialized training and equipment in order to combat such a technical war.

Lastly, tapping all government allied agencies at the regional and international level will enhance capacity building efforts.

V. RECOMMENDATIONS

1. A law on cybercrime be enacted without delay, to supplement RA 8792, which conforms to internationally accepted standards.

2. Create a special agency with the technical expertise to monitor and regulate cyber-activities.

3. Law enforcement agencies be manned by law enforcement personnel with adequate computer skills and technical expertise and thoroughly trained to operate highly technical equipment.

4. Adequate resources be provided to law enforcement agencies in order to acquire the necessary tools, equipment and technical skills and continuously upgrade them for the defence of network systems from cybercrime attacks.

5. Technologies like firewalls, encryption and other infrastructure systems be required for all computer network systems in order to prevent intrusions.

6. Co-operation among all sectors of society to combat cybercrime.

7. Advocacy to increase awareness of the dangers of cybercrime be strengthened to include public awareness in order for everyone to become responsible and ethical users of computers and information systems.

8. Continuous efforts to lobby the members of Congress for the immediate passage of the cybercrime bill, to include the problem of cyber-terrorism.

9. Capacity building measures to ensure that law enforcement officers have a wide array of technical expertise in pursuing cybercrime-related investigations.

10. Technical equipment must also be updated, as technology is rapidly changing, in order to cope with the modern equipment of today's cybercrime offenders.

11. International co-operation like the MLAT must also be strengthened in order for member countries to address the problem of cybercrime.