

“The Legal Framework on Cybercrime and Law Enforcement in Mexico”

Contribution to the Second WSIS Action Line C5 Facilitation Meeting

**Version 1.0
May, 2007**

By

Cristos Velasco*

* Director General, North American Consumer Project on Electronic Commerce (NACPEC) www.nacpec.org

TABLE OF CONTENTS

I. General Background	3
II. International Fora Membership	4
III. International Cooperation	4
IV. National Computer Emergency Response Team (CERT)	4
V. Application of Substantive Criminal Law in the Area of ICTs	5
1. Theft	5
2. Fraud	6
3. Forgery	6
4. Offences Related to Corruption of Minors and Child Pornography	7
5. Offences Related to Sexual Tourism of Minors	8
6. Crime of Pandering (Lenocinio)	8
7. Offenses Related to Financial Payment Systems	9
A. Misuse of Payment Systems	9
B. Illegal Electronic Transfer of Funds	9
8. Offences Related to Interception of Private Communications	9
A. Federal Law Against Organized Crime	10
a. Activities Subject to Intervention	10
b. Exemptions	10
c. Sanctions and Penalties	10
9. Offences Related to Disclosure of Secrets	10
10. Offences Related to Computer and Systems	11
11. Offences Related to Infringement of Copyrights	11
VI. State Legislation	12
VII. Law Initiatives on Cybercrime	12
VIII. Cybercrime Law Enforcement	13
1. The National Cybercrime Police Unit	13
2. DC Mexico	14
IX. Conclusion	14

The Legal Framework on Cybercrime and Law Enforcement in Mexico

I. General Background

Mexico, like most developing countries is starting to take the issue of cybersecurity more seriously as more citizens connect to the Internet, carry financial transactions and make use of government related services online. Mexico does not currently have special rules to combat illicit crime conducted through the Internet. However the existing framework, which is mostly contained in the Federal Criminal Code (hereinafter “FCC”) applies to the criminal conduct committed in cyberspace.

In the international arena, Mexico has been very proactive participating in international organizations and enforcement groups in the area of consumer protection policy on electronic commerce like the OECD Committee on Consumer Policy (CCP) and the International Consumer Protection Enforcement Network (ICPEN). However, in the area of security and cybercrime, participation from the national criminal law enforcement groups remains conspicuously absent, and there are a number of issues, particularly international cooperation with other law enforcement groups that need to be addressed so as to provide legal certainty and security to Mexican Internet users.

The purpose of this background paper is to give an updated overview of Mexico’s legal framework to prevent and combat cybercrime, and the activities of the existing law enforcement groups. This paper will analyze the current provisions contained in the FCC and other laws in different areas of cybercrime, namely illicit access to computer systems, theft, fraud, forgery, corruption of minors and child pornography, offences related to financial payment systems, interception of private communications, disclosure of secrets, offences related to infringement of copyrights and state legislation. The work of the national emergency response team and law enforcement authorities will also be the subject of our analysis.

This paper is submitted as a contribution to the Second WSIS Action Line C5 Facilitation Meeting on Cybersecurity organized by the ITU in Geneva, and it aims to share information on the status of cybercrime legislation and law enforcement, as well as to feed into the international cooperation activities and work of the *Strategy and Policy Unit of the ITU* and other multilateral and regional organizations working in the area of security of networks and cybercrime like the *Cybercrime Convention Committee of the Council of Europe*, the *OECD Working Party on Information Security and Privacy*, the *Telecommunications and Information Working Group of APEC*, and the *Intergovernmental Group of Experts on Cybercrime of the Organization of the American States*.

Likewise, this paper seeks to serve not only as a national reference material for the legal frameworks area, but also to foster awareness on the urgent need to address the issue of cybersecurity and cybercrime among the law enforcement agencies, government and industry groups at the national level.

II. International Fora Membership

Mexico is a member country of the following international organizations currently working on issues related to the prevention of cybercrime, security and data privacy:

A. Through the Direction General of Digital Economy of the Ministry of Economy (*Secretaría de Economía SE*) is part of the OECD's Working Party on Information Security and Privacy (WPISP), the mandate of which includes the promotion of a culture of security in the design and use of ICT's and take steps to enhance the security of information system and networks, and the protection of privacy and personal data in OECD countries.¹

B. The Direction General of Digital Economy of the Ministry of Economy is also part of APEC's Electronic Commerce Steering Group (ECSG), which part of its mandate includes the development of adequate information privacy and data protection, ensuring the free flow of information and the development and use of electronic commerce in the Asia-Pacific region.²

C. The Federal Telecommunications Commission (*Comisión Federal de Telecomunicaciones Cofetel*) is part of APEC's Telecommunications and Information Working Group (APEC-TEL). Such working group has issued a Cybersecurity Strategy, consisting of a package of security measures to protect business and consumers from cybercrime, and to strengthen consumer trust in the use of electronic commerce.³

D. The Ministry of Foreign Affairs (*Secretaría de Relaciones Exteriores SRE*) represents Mexico at the Organization for American States (OAS), forum where there is an Intergovernmental Group of Experts on Cybercrime. The mandate of the said group includes the preparation of inter-American legal instruments and model legislation for the purpose of strengthening hemispheric cooperation in combating cybercrime, considering standards relating to privacy, the protection of information, security, procedural aspects, and crime prevention.⁴

III. International Cooperation

Mexico has not signed the *Council of Europe Cybercrime Convention (COE)*, and as far as the author is concerned, no government efforts have been taken in order to become a party to such convention. Although Mexico is not a party to the *COE Cybercrime Convention*, it has criminal legislation in force that may also apply to combat illicit conduct committed on cyberspace as mentioned in section V of this paper.

IV. National Computer Emergency Response Team (CERT)

The General Direction of Computing Academic Services of the National Autonomous University of Mexico (DGSCA-UNAM) proposed in 2000 the creation of a CERT team in

¹ OECD's WPISP website is available at:

http://www.oecd.org/document/46/0,2340,en_2649_34255_36862382_1_1_1_1.00.html

² APEC' ECSG website is available at:

http://www.apec.org/apec/apec_groups/som_special_task_groups/electronic_commerce.html

³ APEC-TEL website is available at:

<http://www.apectelwg.org/>

⁴ OAS's Intergovernmental Group of Experts on Cybercrime is available at:

<http://www.oas.org/juridico/english/cyber.htm>

order to function as a national contact point for the dissemination of information and responses to network security incidents under the domain name unam.mx. In 2001, the Steering Committee of the Forum of Incident Response and Security Teams (FIRST)⁵ officially granted (DGSCA-UNAM) the approval to operate as a national CERT.

UNAM-CERT⁶ has a website, and as part of its security awareness activities, it disseminates information and newsletters containing technical information, security measures and vulnerabilities of computer software, as well as a section with relevant news and updates on such topics. UNAM-CERT holds an annual congress on security with the purpose to share the latest tendencies on information and networks security with a wide range of international and national participants from the public, private and academic sectors.

V. Application of Substantive Criminal Law in the Area of ICTs

In Mexico, illicit conduct committed through the use of the Internet, electronic means or with the support of computer equipment or systems is punishable pursuant the current provisions of the FCC, which is a federal legislation in force across the Mexican Republic. This section analyses the crimes and the current provisions applicable to those illicit activities carried out through the use of computer systems and the Internet.

1. Theft

The FCC contains a specific chapter on ‘*Theft*’ (within Book Second, title Twenty Second entitled: “*Crimes Against the Patrimony of the Persons*”) consisting of 21 articles, which punishes the crime of theft, and that may also be applicable to illicit activities online. Among the most relevant provisions of that chapter are the following:

“Article 367. Theft is committed when an individual takes possession of personal or movable property belonging to another person without his right and consent that may make use of such pursuant the law”.

“Article 368bis. A sanction from three to ten years imprisonment and a penalty of one thousand days of salary shall be imposed on the person who, after the execution of the theft and without having taken part possesses, alienates in any form, obtain, receives the instruments, items or products resulting from the theft knowing such circumstance and the intrinsic value of such is above 500 times the minimum salary⁷”.

“Article 368 Ter. A sanction from six to thirteen years of imprisonment, and a penalty of one hundred to one thousand days shall be imposed to the person who commercializes theft objects in a habitual manner knowing such circumstance, and the intrinsic value of the said objects is higher than 500 times the minimum salary”.

⁵ FIRST website is available at: <http://www.first.org/>

⁶ UNAM-CERT team is one of the three existing academic CERT’s in Latin America. The other two are located in Chile and Brazil. UNAM-CERT website is available at: <http://www.cert.org.mx/>

⁷ The monetary fines contained in the FCC are referred to and express in Minimum Salary Days (*Días de Salario Mínimo*). Currently, a “*Minimum Salary Day*” consists of eight working hours equivalent to an amount of \$50.57 (Fifty Mexican pesos 57/100) (EUR 3.37) depending on the activity of the worker and the geographic area where he is located, see *Comisión Nacional de Salarios Mínimos* at: <http://www.conasami.gob.mx/>. (Last visited May 10, 2007)

“Article 369. For the application of a punishment, theft shall be considered as executed from the moment a thief is in possession of the stolen object; even when he dispossesses or abandons it. With regard to the fixing of the value of theft, as well as the assertion of a penalty, the salary at the time of the execution of the theft shall be taken into consideration”.

“Article 370. When the value of theft does not exceed one hundred times the salary, a sanction of up to two years imprisonment and a fine of one hundred times the salary shall be imposed.

When the value of theft exceeds one hundred but not five hundred times of salary, the sanction shall be from two to four years imprisonment and a fine of one hundred until one hundred eighty times the salary.

When the value of theft exceeds five hundred times of salary, the sanction shall be from four to ten years imprisonment and a fine of one hundred eighty until five hundred times the salary”.

2. Fraud

The FCC does not expressly provide punishment for computer or Internet related fraud, however the FCC contains a specific chapter on ‘*Fraud*’ (Chapter III within Book Second, title Twenty Second entitled: “*Crimes Against the Patrimony of the Persons*”) consisting of six articles; among the most relevant provisions of this chapter are the following:

“Article 386. The crime of fraud is committed by the person who has misled someone or has taken advantage of the error a person has committed by illegally obtaining a thing or reaching an undue profit.

The crime of fraud is punishable with the following penalties:

I. Imprisonment from 3 to 6 months or 30 to 180 days of fine when the value of the defrauded amount does not exceed ten times the salary.

II. Imprisonment from 6 months to 3 years and 10 to 100 days of fine when the value of the defrauded amount exceeds of 10 but not of 500 times the salary.

III. Imprisonment from 3 to 12 years and fines up to 120 times the salary if the value of the defrauded amount exceeds 500 times the salary”.

Article 387 contains other hypothesis and scenarios whereby fraud is considered as executed, however none of these hypotheses expressly provide the punishment of “*electronic fraud*”. Those hypotheses would very likely be applied when the fraud involves, money, contracts, material things, merchandise and in general goods that are considered personal patrimony of an individual.

3. Forgery

The FCC contains a chapter on ‘*Document Forgery*’ (Chapter IV within Book Second, title Thirteenth, entitled: “*Falsity of Documents in General*”) consisting of four articles.

“Article 243. The crime of Forgery of public documents shall be punished with imprisonment from four to eight years and a fine from two hundred to three hundred sixty days. In the case of private documents with imprisonment from six months to five years and a fine from one hundred eighty to three hundred sixty days.

If the person that executes the forgery is a public official, the punishment will be increased up to a double”.

Article 244 of the FCC contains a list of criteria in ten sections of what shall be considered as forgery. Among these are: (i) including a false signature; (ii) used a blank signature pertaining to another person; (iii) modify the text of a document after its conclusion and execution; (iv) change a date or any other circumstance of time in a document; (v) attribute a name, title, capacity or circumstance for the validity of a document or legal act; (vi) draft a document that changes the terms, rights and obligations of an agreement; (vii) add or modify false facts in a document to be used as evidence in trial; (viii) issuing a testimony based on false premises; (ix) modify the content of a translated document from a legal, technical or science expert; (ix) issue plates, ID’s or any other official identification without the authorization of the correspondent authority.

Article 245 provides the hypothesis in order for a crime of document forgery to be considered as such and punished, such hypothesis could be: (i) that the falsifying individual seeks to take advantage for himself or for another or to cause detriment to society, the state or a third party; (ii) that the falsification resulted in detriment of society, to the state or a private individual either in his belongings, in his person, in his honor or in his reputation. (iii) that the falsifying individual executes the forgery without consent of the person seeking to cause detriment.

Article 246 contains a list of professionals and civil servants that may fall in the hypothesis provided in article 243. These could be: public officials, employees, public notaries, doctors and employees of the telecommunications and radio industries.

4. Offences Related to Corruption of Minors and Child Pornography

The FCC expressly punishes the corruption of minors and child pornography in articles 202 to 203 BIS. The punishment of these conducts also applies to online activities or through the use of networks, computer and electronic systems. The provisions are the following:

“Article 202. The crime of pornography with individuals younger than eighteen years or with persons who do not have the capacity to understand the meaning of the fact or of persons who do not have the capacity to avoid it, is committed when someone procures, obliges, facilitates or induces by any mean to one or several of such persons to perform sexual acts or of corporal exhibitionism with lascivious or sexual purposes, real or simulated with the purpose to record, photograph, film, exhibit or describe them through printed advertisements, transmission of data archives in a public or private telecommunications network, computer systems, electronics or substitutes. An imprisonment from seven to twelve years and a fine from eight hundred to two thousand days shall be levied to the author of this crime.

An imprisonment from seven to twelve years and a fine from eight hundred to two thousand days, as well as the confiscation of the materials, instruments and products of the illicit conduct shall be levied to the person who fixes, prints, records, photographs, films or describes sexual acts of corporal exhibitionism or lascivious or sexual, real or simulated where one or several individuals younger than eighteen years or one or several individuals who do not have the capacity to understand the meaning of the fact or one or several individuals who do not have the capacity to avoid it participate. The same punishment shall be levied upon to the person that

reproduces, stocks, distributes, sells, buys, leases, exposes, advertises, transmits, imports or exports the material referred to in the above mentioned paragraphs.”

Article 202 BIS provides an imprisonment from one to five years and a fine from one hundred to five hundred days to the person who stocks, acquires, and leases the material referred to in article 202 without commercialization or distribution purposes. Likewise, the person shall be subject to specialized psychiatric treatment.

5. Offences Related to Sexual Tourism of Minors

The FCC, contains a special chapter titled: “*Sexual Tourism Against Persons Younger than Eighteen Years Old or of Persons Who Do Not Have the Capacity to Understand the Meaning of the Fact or of Persons Who Do Not Have the Capacity to Avoid it*”. Such chapter punishes sexual tourism activities in national territory, and consists of articles 203 and 203 BIS as follows:

“Article 203. The crime of sexual tourism is considered as such when a person through any means promotes, publishes, invites, facilitates or arranges to one or more persons to travel into the interior or the exterior of the national territory with the purpose to have any kind of real or simulated sexual acts with one or more persons younger than eighteen years or with one or several individuals who do not have the capacity to understand the meaning of the fact or with one or several individuals who do not have the capacity to avoid it.

An imprisonment from seven to twelve years and a fine from eight hundred to two thousand days shall be levied to the person who commits this crime”.

“Article 203 BIS. An imprisonment from twelve to sixteen years and a fine from two thousand to three thousand days shall be levied to the person who performs any kind of real or simulated sexual acts with one or more persons younger than eighteen years, or with one or several individuals who do not have the capacity to understand the meaning of the fact or with one or several individuals who do not have the capacity to avoid it, by virtue of sexual tourism. Likewise, the person shall be subject to specialized psychiatric treatment”.

6. Crime of Pandering (Lenocinio)

The FCC, contains a chapter titled: “*Pandering of Persons Younger than Eighteen Years Old or of Persons Who Do Not Have the Capacity to Understand the Meaning of the Fact or of Persons Who Do Not Have the Capacity to Avoid it*”. Such chapter consists of article 204, which mentions:

“Article 204. The crime of pandering of persons younger than eighteen years, or of individuals who do not have the capacity to understand the meaning of the fact or of individuals who do not have the capacity to avoid it is committed when:

- I. Any person exploits the body of any of the individuals before mentioned through carnal trade or by obtaining of any profit;*
- II. The person induces or requests to any of the individuals before mentioned to sexually trade their body or through the facilitation of the means for prostitution; and*
- III. To the person that manages, administers or directly or indirectly maintains brothels, prostitutions houses or other places devoted for prostitution exploitation of persons younger than eighteen years, or of individuals who do not have the capacity*

to understand the meaning of the fact or of individuals who do not have the capacity to avoid it, and obtains any benefit with his outcome.

An imprisonment from eight to fifteen years and a fine from one thousand to two thousand five hundred days shall be levied to the person responsible for this crime, as well as the definite closing of the places described in section III”.

7. Offenses Related to Financial Payment Systems

A. Misuse of Payment Systems

The commercialization and misuse of credit and debit cards and in general of any instruments of payment used by the banking and financial systems, as well as the illicit access and hacking of computer systems pertaining to the financial and banking systems is punishable under article 112 Bis of the Law of Credit Institutions (LCI), which textually provides:

“Article 112 Bis.- A sanction from three to nine years imprisonment and a fine of thirty thousand to three hundred thousand days of salary shall be levied upon the person who:

I. Produces, reproduces, introduces into the country, prints or trades debit and credit cards, check formats or drafts or in general payment instruments used by the banking system without the consent of the person with the power to do so;

II. Possesses uses or distributes debit and credit cards, check formats or drafts or in general payment instruments used by the banking system knowing they are fake;

III. Modifies the electronic identification and accesses electromagnetic equipment of the banking system with the purpose to obtain economic resources unduly; and

IV. Unduly obtains or uses information about customers or transactions of the banking system without having the corresponding authorization.

The corresponding punishment may be increased up to a half more, when the person who carries any of the activities provided in the afore mentioned clauses has the capacity of counsel, functionary or employee of any credit institution.”

B. Illegal Electronic Transfer of Funds

Access to monetary or security resources pertaining to customers of credit institutions through illegal schemes on the internet such as phishing, pharming or identity theft may be punished under article 113 Bis of the LCI, which textually provides:

“Article 113 Bis.- A sanction from three to ten years imprisonment and a fine of five hundred to thirty thousand days of salary shall be levied upon the person who unduly uses, obtains, transfers or in any other form obtains securities or resources from customers of credit institutions.

If those that commit the crime described above are functionaries or employees from credit institutions or third parties with authorized access to the systems of such institutions, the punishment shall be from three to fifteen years imprisonment and a fine of one thousand to fifty thousand days of salary.”

8. Offences Related to Interception of Private Communications

Articles 16 to 28 of the Federal Law Against Organized Crime (FLAOC) provide the legal hypothesis, modalities and procedures to authorize the interception of private communications by judicial authorities in national territory.

A. Federal Law Against Organized Crime

Article 16 of the FLAOC establishes that when an intervention of private communications is deemed as necessary by the Attorney General or the head of the specialized unit, it shall be requested in writing from the District Judge indicating the purpose and need of the intervention, the information assuming that in the investigation of crimes involves a member of the organized crime, as well as the facts, circumstances, data and other elements seeking to be proofed. The intervention requests shall additionally include the person or persons to be searched, the identification of the place or places to be seized, the type of private communication to be intervened, its term, the procedure and equipments for the intervention, and where applicable, the identity of the person who will render the service through which the communication intervention is carried.

a. Activities Subject to Intervention

The third paragraph of article 16 of the FLAOC establishes that the following activities are subject to intervention of private communications: those carried out orally, in writing, by signs, signals or through the use of electrical, electronic, mechanic, wired and wireless devises, computing and equipment systems, as well as by any other mean or form allowing the communication between one or multiple emitting parties or one or multiple receiving parties.

b. Exemptions

Article 17 of the FLAOC stipulates that the district judge might not be able to authorize interventions when dealing with electoral, tax, mercantile, civil, labor or administrative matters, and neither those communications between an individual under arrest with his defense.

c. Sanctions and Penalties

Article 28 of the FLAOC establishes that those taking part in an intervention of private communications shall keep the reserve of their content. Public servants of the specialized unit, as well as any other public officials of the Federal Power of the Federation involved in any procedure of the crimes referred to in the FLAOC that disclose, inform or unduly use in detriment of another information or images obtained in the course of an intervention of private communications, whether or not it was authorized shall be punished with imprisonment from six to twelve years, a fine tantamount to five hundred days of salary, as well as the removal to develop another job, charge or public commission for the same term of the imprisonment punishment levied upon. The same punishment shall be levied upon those that have knowledge of the existence of a petition or authorization of interventions of private communications, and disclose their existence or content as a result of their job, charge or public commission.

9. Offences Related to Disclosure of Secrets

Article 211 BIS of the FCC punishes the disclosure of information or images obtained as a result of an intervention of private communications in detriment of an individual with an imprisonment term from six to twelve years and a fine from three hundred to six hundred days of salary.

10. Offences Related to Computer and Systems

The FCC contains a full chapter prohibiting and sanctioning illegal access to computer equipment and information technology systems. These federal offences are prosecuted as a result of an individual petition of the victim to the federal authorities (*querrela de parte ofendida*). Title Nine, chapter II of the FCC consists of seven articles 211 bis 1 to 211 bis 7 entitled '*Illegal Access to Systems and Informatics Equipment*'.

Articles 211 bis 1 to 211 bis 7 establish imprisonment from two to eight years and fines from 100 days to 900 days to: (i) those that modify, destroy or cause the loss of information contained in computing and systems equipment '*protected by a security mechanism*' pertaining to particulars or to the state or to financial institutions; and (ii) those who know or copy information contained in computing and systems equipment pertaining to particulars or to the state or to financial institutions, and '*protected by a security mechanism without an authorization*'. The penalties and imprisonment sanctions contained in those provisions may be doubled when government officials and employees of the state and staff of financial institutions make the conduct or when the information obtained is used for personal illicit purposes.

11. Offences Related to Infringement of Copyrights

Title Twenty-Six of the FCC contains the legal hypothesis and crimes in the area of copyright. The offences contained in such title are prosecuted as a result of an individual petition of the victim to the federal authorities (*querrela de parte ofendida*) except for section I of article 424 -with regards to the speculation of the publication of free text books distributed by the Mexican government-, which is prosecuted by the authorities without the need for an individual petition (*de oficio*).

Article 424 section III provides imprisonment from six months to six years and a penalty from three hundred to three thousands days of salary to the individual who illegally uses works protected under the Federal Law of Author Rights (FLAR) with the intention to profit and without the corresponding authorization.

Article 424 bis provides imprisonment from three months to ten years and from two thousand to twenty thousands days of fines to: (i) individuals who produce, reproduce, introduce into the country, stock, transport, distribute, sell or lease copies of works, phonograms, videos, books protected under the FLAR in an illegal form, with commercial purposes and without the authorization of the party entitled to the rights of the author or related rights pursuant to the FLAR; (ii) to those who know, provide prime sources and materials destined to the production or reproduction of works, phonograms, videos, books referred in the aforementioned paragraph; or (iii) to the individual who manufactures a device or system with the intention to profit, the purpose of which is to deactivate electronic protection devices of a computing program.

Article 424 ter provides imprisonment from six months to six years and a penalty from five thousand to thirty thousands days of salary to the individual who sells copies of works, phonograms, videos or books to a final consumer in public spaces, illegally and with commercial speculation purposes.

Article 425 stipulates imprisonment from six months to two years or a fine from three hundred to three hundred thousands days of salary to the individual who knows and exploits an interpretation or execution with commercial purposes and without any right.

Article 426 contains imprisonment from six months to four years and a fine from three hundred to three thousand days when the following hypothesis occur: (i) to he who manufactures, imports, sales or leases a devise or system to deactivate a satellite signal, a program database without authorization of the legitimate distributor of such signal; and (ii) to he who carries out any act with the purpose to deactivate a satellite signal or a program database without authorization of the legitimate distributor of such signal and with profiting purposes.

Article 427 stipulates imprisonment penalties from six months to six years and a fine from three hundred to three thousands days to the person who publishes a work substituting the name of the author for another name.

Article 428 provides that the monetary penalties provided in this title shall be applied regardless of the redress damage, amount of which may not be lower than forty per cent of the final sale price to the public for each product or as a result of the rendering of services involving a breach of one or of any of the rights provided in the FLAR.

VI. State Legislation

Sinaloa, a state located North-West of Mexico was the first state to regulate and punish cybercrime in the Mexican Republic. Article 217 of the Criminal Code of that state provides the following:

“Article 217. A person illegally and without any right commits a cybercrime when:

I. Uses or accesses a database, computer systems or computer networks or any part thereof with the purpose to design, execute or amend an scheme or device with the intention to defraud, obtain money, goods or information; or

II. Intercepts, intervenes, receives, uses, modifies, damages or destroys a logical support or computer program, or the data contained thereof, in the base, system or network.

A punishment from six months to two years imprisonment, and fines from ninety to three hundred days of salary shall be levied upon to the responsible of a cybercrime”.

VII. Law Initiatives on Cybercrime

Since 2000, the Mexican Congress has organized seminars and workshops with different stakeholders in order to find paths to reform the FCC, and include offences and punishment of Internet related crime. However, due to the complexity of the subject, and particularly the fact that the FCC and other laws currently apply to criminal activities conducted through the use of ICTs and computer equipment; the Mexican Congress found that there was no need for a new reform to the FCC. However, efforts are now focused in finding better enforcement and cooperative measures among the national administrative and judicial authorities in order to prosecute criminal activities conducted in cyberspace.

VIII. Cybercrime Law Enforcement

1. The National Cybercrime Police Unit

Mexico's Cybercrime Police Unit (hereinafter "MCPU") was created in 2000 and functions under the umbrella of the Ministry of Public Security⁸. MCPU has a specific area for the prevention and attention of child related crimes such as pornography and pedophiles.

MCPU gives priority to the following four objectives: (i) identification and dismantlement of organizations devoted to theft, traffic, child corruption and the distribution of child pornography on the internet; (ii) localization and arrest of individuals involved in cybercrimes and brought to the attention of competent authorities; (iii) internet supervision and patrolling in order to track hackers, criminals and organized crime; and (iv) research and analysis on national and international activities to prevent and track pedophile and child prostitution networks.

In order to foster a culture of reporting cybercrime for internet users in Mexico, MCPU launched a telephone line and an e-mail address that affected individuals can use to submit and report internet related frauds and crimes. The complaints are resolved on a first come first serve basis. Likewise, MCPU frequently participates in seminars and meetings in order to foster education and awareness on cybercrime issues in Mexico.

Statistics from the Direction General of the MCPU as of October 2006 show that 1,229 related complaints on electronic commerce were pursued with a defrauded amount equivalent to 2 million Mexican pesos.⁹

Complaints Pursued by the Cybercrime Police Unit (Until October 2006)

Source: Direction of the Cybercrime Police and Crimes Against Minors of the Ministry of Public Security

E-Commerce fraud	583
Threats	120
Online Banking Fraud	94
Cybercrime	85
Crimes against Minors	78
Phishing	58
Hacking	54
Online Fraud	49
Slander	42
Online Patrolling	25
Illegal websites	16
Spam	15
Extortion	5
Mail Tracking	1
Equipment theft	1
Prostitution	1
Cyber terrorism	1
Sexual Harassment	1
Total	1,229

⁸ The website of Mexico's Cybercrime Unit is available at: <http://www.ssp.gob.mx>

⁹ Profeco, " *El lado oscuro de Internet* ", Boletín Brújula de Compra No. 28, (November 13, 2006), available at: http://www.profeco.gob.mx/encuesta/brujula/bruj_2006/bol28_internet.asp

2. DC Mexico

In December 2002, the Ministry of Public Security through the *Cybercrime Police Unit* formed a multidisciplinary enforcement and prevention group known as Cybercrime-Mexico (“*DC Mexico*”).¹⁰ DC Mexico is led by the *Cybercrime Police Unit* as the technical secretariat, and is formed of government entities of the Federal Executive, Legislative and Judicial Power through representatives from the Senate and the Chamber of Deputies, state governments, telecommunications companies and ISPs rendering computer security services, academic institutions, industry chambers and associations and civil society groups. The purpose of DC Mexico is to identify, track and locate illicit conduct on the Internet affecting individuals in national territory, and to foster a culture of respect, security and legality in Mexico.

DC Mexico holds meetings on a regular basis, and is subdivided into various divisions and working groups that carry out specific Internet security tasks and periodically report on their activities. Among these working groups are: the informatics contingency subgroup; the training and new technologies subgroup; the government subgroup; and the legal experts group. DC Mexico serves as the official point of contact with other cybercrime units across US and Europe that form a collaborative combat network known as the “*24x7 Point of Contact Network*,” which is an international alliance of countries with cybercrime units that mutually cooperate to monitor the security of the internet. DC Mexico also works very closely with US customs authorities and has established close links with the US Secret Service and the Technological Brigade of Spain.

DC Mexico has done a fairly good job in preventing crime and illicit conduct on the Internet, and particularly in the fight against child corruption and pornography. The security and telecommunication corporations part of DC Mexico constantly provide information to the online community about the latest virus and worm attacks and they seek to foster the use of means and technical tools for companies, academic institutions and consumers to prevent and combat cybercrime in Mexico.

IX. Conclusion

Due to the borderless nature of the Internet and considering that cybersecurity is a global issue that requires coordination and international cooperation among law enforcement agencies, Mexico should be more proactive in the international arena by participating, following and implementing the policy recommendations arising from multilateral and regional organizations working on cybercrime at the local level, and should also consider the adoption of the *COE Cybercrime Convention*. The adoption of such instrument would not only lead to a general reform of the adjective and substantive criminal legislation, but it would also strengthen the existing legal framework, help to improve security measures at the local level, and develop a much closer international coordination with law enforcement groups from other countries to combat cybercrime more effectively.

The fight against cybercrime in Mexico is built upon the legal framework contained in the FCC, the LCI and the LAOC, and the corresponding enforcement by the offices of the federal attorney general, state attorneys and the cybercrime unit.

¹⁰DC Mexico’s activities are available in the website of the Ministry of Public Security at: <http://www.ssp.gob.mx/>

One of the problems that remains to be addressed in order to enforce legislation more effectively and prosecute crimes committed on the Internet affecting Mexican citizens is to develop a comprehensive coordination plan between the federal offices of the attorney general, state attorney generals and the cybercrime unit. Criteria in the interpretation of criminal laws, jurisdiction and competence issues and enforcement collaboration remain challenging tasks.

In the area of information sharing and awareness, Mexico through UNAM-CERT should continue to provide information for evaluating security threats and vulnerabilities and issuing required warnings and patches to the Internet community, as well as coordinating efforts with other CERTs, with the local cybercrime unit and with other international law enforcement groups in order to identify legal and technical issues to prevent cybercrime on a global scale.