Octopus Interface Conference: Cooperation against Cybercrime

Presentation: "General Summary of the Legal Framework concerning Cybercrime and Law Enforcement in Mexico"

Cristos Velasco, Director General
North American Consumer Project on Electronic Commerce (NACPEC)

Council of Europe
Strasbourg, France
11 June 2007

Ladies and gentleman, distinguished guests, and fellow participants, thank you for the opportunity to provide a perspective on the legal framework concerning cybercrime and law enforcement in Mexico. I'd like to thank the Directorate General of Human Rights and Legal Affairs of the Council of Europe. I thank Mr. Alexander Seger and his friendly staff for the invitation to make a brief presentation on a paper originally submitted to the Second WSIS Action Line C5 Facilitation Meeting on Cybersecurity organized by the International Telecommunications Union ITU in Geneva on May 14-15, 2007.

We believe that the use of the Cybercrime Convention and its Protocol on Xenophobia and Racism will not only be used as a cooperation instrument among the countries to combat cybercrime on a global scale but it will also serve as a set of guidelines for the development of national legislation, especially in those countries that do not yet have legislative frameworks in place to combat cybercrime and the growth and evolution of other Internet related threats affecting end users.

Please note that this paper does not represent an official position of the government of Mexico. Nevertheless, our paper offers an updated overview of the applicable legal framework for preventing and combating crimes committed in cyberspace, and of the activities of existing law enforcement groups to tackle cybercrime issues in Mexico. In general, this paper aims to feed into the international cooperation activities and work of other multilateral and regional organizations working in the area of security of networks and cybercrime such as the *Cybercrime Convention Committee of the Council of Europe*, the *Strategy and Policy Unit of the ITU*, 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.*

I will now proceed to provide a brief summary of the most relevant provisions on computer and Internet related crime found in the Federal Criminal Code and the Federal Law of Credit Institutions (FLCI) and will also briefly talk about the work and challenges of the existing law enforcement groups in Mexico.

In the Area of Financial Payments

Article 112 of the FLCI provides punishment of three to nine years imprisonment and monetary fines from EUR 100,000 to EUR 1'000, 000 to the person who modifies electronic identification and accesses electromagnetic equipment of the banking system with the purpose of obtaining economic resources unduly; and obtains or uses information about customers or transactions of the banking system without corresponding authorization.

Article 113 Bis of the FLCI provides a punishment sanction from three to ten years imprisonment and monetary fines from EUR 1,670 to EUR 100,000 to the person who unduly uses, obtains or transfers securities or resources from customers of credit institutions. The penalties described above may be increased up to one-half more when counsel, functionaries and employees from credit institutions carry out such activities.

In the Area of Illicit Access to Computers and Systems

The FCC contains a full chapter prohibiting and sanctioning illegal access to computer equipment and information technology systems. The offences are prosecuted as a result of an individual petition of the victim to the federal authorities (*querella de parte ofendida*).

Articles 211 bis 1 to 211 bis 7 establish imprisonment penalties from two to eight years and monetary fines from EUR 335 to EUR 3,000 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, 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 carry out the conduct or when the information obtained is used for personal illicit purposes.

In the Area of Copyrights Infringement

The FCC contains a full chapter on offences against author's rights. One of the most relevant provisions of this chapter is:

Article 426, which contains imprisonment punishment from six months to four years and monetary fines from EUR 1,000 to EUR 10,000 when the following hypothesis occur: (i) when an individual manufactures, imports, sales or leases a device or system to deactivate a satellite signal or a program database without authorization of the legitimate distributor of such signal; and/or (ii) a person who carries out activities 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.

In the Area of Child Pornography

The FCC contains a chapter (articles 202 and 203 BIS) that punishes the conduct of Child Pornography and the dissemination and transmission of material through public or private telecommunications networks, or computer and electronic systems. Imprisonment from seven to twelve years and monetary fines from EUR 2,700 to EUR 6,700 are levied to the individual committing such offenses, as well as those who help to fix, print, record, photograph, film or facilitate child pornography. Likewise, article 202BIS of the FCC provides an imprisonment from one to five years and monetary fines from EUR 340 to EUR 1,670 to the person who stocks, acquires, and leases child pornography material referred to in article 202 including material contained in computer and electronic systems.

Articles 203 of the FCC punishes sexual tourism activities with minors and its promotion in national territory with imprisonment terms from seven to twelve years and monetary fines from EUR 2,670 to EUR 6,700. Article 203 BIS expressly punishes the conduct of sexual activity with minors as a result of sexual tourism with imprisonment from twelve to sixteen years and monetary fines from EUR 6,700 to EUR 10,000.

Additionally, the Federal Criminal Code provides punishments and monetary fines for traditional forms of crime such as theft, fraud, and document forgery. The Federal Law against Organized Crime punishes offences related to the interception of private communications and the disclosure of information, images and secrets by judicial authorities, resulting from the intervention of private communications.

In the Area of Law Enforcement

Mexico has a Cybercrime Police Unit, which has been operating under the umbrella of the Ministry of Public Security since the year 2000. The Cybercrime Police Unit has focused its work on the enforcement of child pornography, corruption of minors and the prosecution of pedophile-organized gangs operating both, on the Internet and within national territory.

The Cybercrime Police Unit 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 bringing this 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.

I was recently informed about the formation of a new incident response group known as “e-Crime Mexico Group”. The e-Crime Mexico Group is a multidisciplinary effort with the principal mission of preventing and reducing cybercrime in Mexico. The tasks of this group include *inter alia*: (i) identifying, monitoring and prosecuting Internet related crimes including fraud, phishing, identity theft and all those crimes involving

information systems; (ii) analyzing and informing about the latest threats to security systems on the Internet; and (iii) fostering a culture of 'information security' in Mexico. The e-Crime Mexico Group will revisit the works originally undertaken by a multidisciplinary enforcement and prevention group formerly known as Cybercrime-Mexico (DC Mexico). Under the lead of the Ministry of Public Security, this taskforce was created in 2002 with the purpose of identifying, tracking and locating illicit conduct on the Internet affecting individuals in national territory.

There are a number of problems that remain to be addressed in order to enforce the existing criminal legislation more effectively and prosecute crimes committed through the use of the Internet. One of the current problems is the lack of coordination and cooperation between the federal offices of the attorney general, state attorney generals and the cybercrime unit. Criteria in the interpretation of federal and state laws, jurisdiction and competence issues and a lack of sufficient financial and human resources remain among those challenging tasks. Also, a detailed coordination plan is urgently needed in order to address these issues among the federal and state attorney generals, the cybercrime law unit, the national CERT and the new e-Crime Mexico group.

We firmly believe that Mexico would benefit from the adoption of the Cybercrime Convention in many ways. First, it would lead to a general reform of the adjective and substantive criminal legislation, and fill in the existing loopholes found in the current criminal laws. In addition, it would lead to the development of a uniform and more cooperative enforcement approach among the federal and local law enforcement authorities and the e-Crrime prevention group.

Thank you very much for your attention. We look forward to continued cooperation on legal issues concerning cybercrime and cybersecurity. We strongly believe that the participation of Mexico in this forum will not only create a path towards the support and adoption of the Cybercrime Convention and its Protocol, but it will also help to improve coordination and cooperation mechanisms at the local level; foster the development of an international network of legal experts and law enforcement groups with international organizations and other countries, and find adequate solutions in building confidence and security in the use of ICTs to the end user.

REFERENCES

Velasco, Cristos, "The Legal Framework on Cybercrime and Law Enforcement in Mexico" Contribution to the Second WSIS Action Line C5 Facilitation Meeting on Cybersecurity organized by the ITU, Geneva (May 11-12, 2007)
http://www.itu.int/osg/spu/cybersecurity/pgc/2007/events/contributions/contribution-to-C5-from-nacpec-14-may-2007.pdf

The NACPEC Website: English http://www.nacpec.org/en/
Spanish http://www.nacpec.org/es/index.html