Web site: www.coe.int/economiccrime

COUNCIL OF EUROPE CONSEIL DE L'EUROPE

Strasbourg, 20 March 2006

T-CY (2006) 06
English only

THE CYBERCRIME CONVENTION COMMITTEE (T-CY)

UNITED STATES ACTIVITIES TO IMPROVE CYBERCRIME LEGISLATION AND INVESTIGATE CAPACITIES

Information submitted by the Delegation of the United States of America

Over the last several years, even before the United States signed the Convention on Cybercrime in November 2001, it began organizing and making available to other countries a number of cybercrime-related programs. These programs have been intended both to assist states in amending their legislation to meet Convention standards (not American law) and to train law enforcement officials, including investigators, prosecutors, and judges, in cybercrime-related issues. This paper describes highlights of recent and projected programs developed or given by the Computer Crime and Intellectual Property Section of the Criminal Division of the Department of Justice (CCIPS).[1]

ACTIVITIES IN THE ORGANIZATION OF AMERICAN STATES

In June 2003, the Group of Government Experts on Cybercrime ("Cybercrime Experts Group") of the Organization of American States (OAS) convened for its third meeting. At that meeting, the group focused its agenda on ensuring that OAS countries had adequate laws to investigate and prosecute cybercrime. The US delegation delivered a presentation highlighting the Cybercrime Treaty of the Council of Europe as the only international instrument that provided a comprehensive legal framework for addressing cybercrime.

Following the June 2003 meeting, and based upon a US proposal adopted by the Cybercrime Experts Group, the group embarked upon a series of four week-long regional workshops intended to provide countries with technical training on drafting and amending their domestic legislation to address cybercrime. The workshops were conducted regionally in an effort to minimize travel expenses and encourage robust participation by countries. The workshops were attended by legislators, senior policymakers, private industry representatives and law enforcement officials from the OAS countries. Each workshop included presentations on the importance of substantive and procedural cybercrime laws that used existing laws from around the world as models. However, the Cybercrime Convention was featured prominently in each workshop, and representatives from the Council of Europe delivered presentations at two of the four workshops to provide information on the treaty and the requirements of accession. The US organized and funded the workshops, but speakers were drawn from many OAS countries.

The first workshop was conducted in January 2004 in Mexico City, Mexico, for Central American countries. It was followed by workshops in Santiago, Chile, and Lima, Peru, for South American countries in September and October 2004, respectively. The last workshop was held in September 2005 for Caribbean countries. In all, almost 200 participants from 29 countries were trained through the workshops.

[1] However, it should be noted that the Federal Bureau of Investigation; the United States Secret Service; the Department of Homeland Security; the Diplomatic Security section of the Department of State; the United States Agency for International Development; and many other US agencies also frequently offer cybercrime-related programs to other countries as budgets permit. These programs normally take place in the requesting country but may sometimes be given in the US. The dozens of programs these agencies have carried out in recent years tend to cover investigative capacity-building matters, such as investigations in electronic networks, cyberforensics, preservation of an electronic crime scene, etc, but may sometimes cover legal or legislative issues. CCIPS often will take part in the programs run by investigating agencies, usually to teach a session on legal issues. In addition, CCIPS runs a periodic coordination meeting with many of these agencies so that all know which countries are being trained by which agencies and on what topics. Interested countries may contact CCIPS for information about how to contact the US investigative agencies.

In December 2005, the OAS and COE held a joint conference that focused upon the Cybercrime Convention and the requirements of accession. The joint conference was an opportunity for the OAS' cybercrime experts to foster stronger relations with the COE's experts and to obtain a firsthand understanding of the Convention's provisions and requirements. The fourth OAS Cybercrime Experts Group meeting held in February 2006 built upon the success of the joint COE/OAS conference. The meeting concluded with the group recommending further exchanges of information between the OAS and COE to assist OAS Countries in deciding whether to accede to the Cybercrime Convention.

At the February 2006 meeting, the OAS also agreed to expand its training by sponsoring additional training, which the United States will develop, on how to develop a computer forensic capability and on how to establish 24-hour-a-day, 7-day-a-week investigative capability relating to cybercrime and other crime involving electronic networks. This program, which will last several days, is being organized for the fall of 2006.

ACTIVITIES IN THE ASIA PACIFIC ECONOMIC COOPERATION FORUM

For the last four years, APEC has sponsored annual cybercrime conferences of experts, organized by the United States, to discuss legislative issues and to improve cooperation between law enforcement agencies responsible for the investigation cybercrime. These meetings have included presentations by speakers from many APEC countries and from the Council of Europe, who have spoken about the Convention.

In addition, as the result of a survey of APEC Member Economies, APEC and the United States funded a project to offer individual countries intensive conferences on the drafting of cybercrime laws to Convention standards. The US organized and provided much of the instruction to the six requesting countries. Each session lasted about a week and took place in the requesting country or nearby. During the life of this project, teams of experts provided direct training and advice to policy makers in the Philippines, Indonesia, Thailand, Peru, Chinese Taipei, and Vietnam. These efforts resulted in the drafting and introduction of new cybercrime legislation.

Under APEC's auspices, the US is now developing other cybercrime-related projects in the area, including training for prosecutors and judges.

ACTIVITIES IN THE MIDEAST AND NORTH AFRICA

In September 2003, a US delegation headed by CCIPS provided a three-day training seminar on legislative drafting in Egypt for the countries of Egypt, the United Arab Emirates, Kuwait, Tunisia, Algeria, Morocco, Jordan, the Palestinian territories, Nepal, Lebanon and Oman. Delegates were provided with background on cybercrime and Internet technologies, instruction on the use of various technologies for investigational purposes, and detailed discussion of how to draft substantive and procedural computer crime laws and mutual legal assistance laws to meet Convention standards. The US delegation also

met individually with the delegations from many of the countries to discuss country-specific concerns or to discuss possible future bilateral assistance in this area.

ACTIVITIES IN SUB-SAHARAN AFRICA

CCIPS is currently planning two cybercrime workshops at the International Law Enforcement Academy ("ILEA") in Gaborone, Botswana, in order to cover many of the countries of the Sub-Saharan African region. The workshops will be held back to back in June 2006 and will each last most of a week. The goals for the workshops are: 1) to provide technical support to participants to assist them in drafting cybercrime legislation to meet Convention standards; and 2) to increase the investigative capacity of the law enforcement community in Africa in regard to electronic networks. Potential attendees will be legislators (or legislative staffers), policymakers (from the government, academia or the local private sector), senior law enforcement officials responsible for drafting and amending cybercrime statutes or for conducting cybercrime investigations, and officers from dedicated cybercrime investigative or prosecutorial units.

CRITIQUES OF DRAFT CYBERCRIME STATUTES

Like many other organizations, CCIPS has been asked by countries that are drafting cybercrime statutes to comment on the drafts. Thus, over the last several years, it has offered confidential comments, usually by email, to about a dozen requesting countries, reviewing as many drafts as a country requests.