PERMANENT COUNCIL OF THE
ORGANIZATION OF AMERICAN STATES

Special Group to Implement the Recommendations
of the Meetings of Ministers of Justice or of Ministers
or Attorneys General of the Americas

OEA/Ser.G
GE/REMJA/doc.51/99
28 October 1999
Original: Spanish

FINAL REPORT
ON THE MEETINGS OF GOVERNMENT EXPERTS ON CYBER CRIME

(Preliminary Version)

FINAL REPORT
ON THE MEETINGS OF GOVERNMENT EXPERTS ON CYBER CRIME

(Preliminary Version)

I. INTRODUCTION

In March 1999 the Ministers of Justice or of Ministers or Attorneys General of the Americas recommended the establishment of an intergovernmental experts group on cyber crime with a mandate to (1) complete a diagnosis of crime targeting computers and information in the member states; (2) complete a diagnosis of national legislation, policies, and practices responsive to such crime; (3) identify national and international entities with relevant expertise; and (4) identify mechanisms of cooperation within the inter-American system to combat cyber crime.

II. BACKGROUND

Toward this end, the First Meeting of Government Experts on Cyber Crime convened in May 1999 to accomplish the goals set out by the ministers of justice or attorneys general. At that meeting, to facilitate fulfillment of its mandate, the group of experts crafted a survey requesting information from each member state about its experience with various types of cyber crime; the substantive laws governing cyber crime; the jurisdiction and extradition principles governing cyber crime; the laws governing the preservation and gathering of evidence in such cases; and the existence of specialized training programs or law enforcement entities and/or experts to combat cyber crime.

Subsequently, the Special Group on Justice decided to hold the Second Meeting of Government Experts on Cyber Crime on October 14-15, 1999.[1/] This meeting was convened to analyze the replies by the governments of member states to the survey on this topic, to consider mechanisms for cooperation on cyber crime within the inter-American system, and to listen to papers presented by the following experts: Dr. Rodolfo Ojales, attorney at the U.S. Department of Justice, Mr. Joe DiAngelo of "Citigroup"; Mr. John Ryan of "America Online"; Mr. Don Cavendar of the "Computer Analysis and Response Team"; Ms. Ketherine Fithen of "Computer Emergency Response Team, Carnegie-Mellon University"; Mr. Steve Branigan of "Bell Labs," and Mr. Raúl Sanguinetti, Head of the Unit, Department of Management Systems. Abstracts of these papers are attached to this report.

With respect to the replies by the governments of member states to the questionnaire crafted at the First Meeting of Government Experts on Cyber Crime (GE/REMJA/doc.15/99)[1/], the Second Meeting had at its disposal a document prepared by the Secretariat for Legal Affairs of the General Secretariat (GE/REMJA/doc.47/99), which compiles and correlates the replies to the questionnaire. That document is attached to this report.

It should be noted that the diagnosis requested is based on replies to the survey by 11 member states as of October 14, 1999 and on the deliberations of the Meeting of Experts throughout its working sessions. Although there were only a limited number of replies, the Meeting considered that they reflect the current situation in the Americas in general terms. In addition, the report contains recommendations designed to strengthen the ability of member states to respond to the major public security concerns and challenges created by new technology and

---

1. To date, replies have been received from Mexico (GE/REMJA/doc.15/99 add. 1); United States (GE/REMJA/doc.15/99 add. 2); Ecuador (GE/REMJA/doc.15/99 add. 3); Brazil (GE/REMJA/ doc.15/99 add. 4); El Salvador (GE/REMJA/doc.15/99 add. 5); Costa Rica (GE/REMJA/doc.15/99 add. 6); Peru (GE/REMJA/doc.15/99 add. 7); Argentina (GE/REMJA/doc.15/99 add. 8); Trinidad and Tobago (GE/REMJA/doc.15/99 add. 9); Panama (GE/REMJA/doc.15/99 add. 10); and Venezuela (GE/REMJA/doc.15/99 add. 11).

to continue forging inter-American mechanisms with which to investigate and combat cyber crime.

III. DIAGNOSIS

For the purposes of this diagnosis, "cyber crime" is defined as a criminal activity in which information technology systems (including, *inter alia*, telecommunications and computer systems) are the *corpus delicti* or means of committing an offense.

Seven (7) member states responding to the survey reported that they had not experienced significant harm from cyber crime. Cyber crime is at present perceived as rare, and often is not specifically criminalized under the law. Nevertheless, some member states do punish crimes committed using information technology when such acts are in themselves offenses, such as, for example, fraud, tax evasion, defamation or distribution of child pornography.

In view of this, there is clearly a need to develop, adapt, and harmonize the legislation, procedures, and institutions required to combat the increasing abuse and misuse of computers in member states.

With respect to legislation regarding the gathering of evidence, the authority to trace, collect, preserve, and disclose electronic communications traffic information and computer data is critical to the investigation of cyber crimes. Given that cyber crime is still incipient and difficult to detect, some member states may not have faced the unique problems associated with gathering evidence regarding this kind of offense. Nine (9) responding states do permit the seizure of tangible materials in accordance with established procedures, and also compelling Internet service providers and telecommunications companies to produce subscriber and billing information. However, it appears that in some cases investigators might not be permitted to take other pertinent steps to investigate cyber crime, such as obtaining source and destination information about communications simultaneously with the transmission of those communications, which may be necessary to trace a computer intrusion.

Perhaps the greatest difficulty facing member states is the dearth of investigative and prosecutorial entities with the expertise to investigate or prosecute cyber crimes. Nor is the requisite training available. However, cyber crimes are frequently investigated by units that have not specialized in that field (units investigating organized crime and drug trafficking, for instance, to mention only two). Given that this lack of entities with expertise could impair both domestic and international investigation of cyber crime, developing suitable mechanisms for acquiring such expertise should be one of the priorities in this area.

Very few member states (they include, however, the United States, among the survey respondents) have experienced difficulties related to the global nature of cyber crimes or have made or received requests for international assistance in cyber crime cases. But despite the lack of requests to date, it is not uncommon to trace a cyber crime through computer networks located in a multitude of countries unrelated to the location of the perpetrator or the victim. Thus, the ability to request and to provide international assistance is critical and deserves further examination by states.

It is not clear from the survey results whether issues relating to jurisdiction, extradition, and international cooperation are adequately governed by the member states' specific or generally applicable laws and existing multilateral and bilateral agreements.

Finally, despite the perceived lack of regional harm from cyber crime to date, presentations to the group by representatives of other international bodies, governments, private sector entities and computer security organizations indicate that the cyber crime problem is escalating; which makes it all the more important to ensure that member states are prepared to investigate and prosecute cyber crime when it arises in their jurisdictions.

IV: IDENTIFICATION OF NATIONAL AND INTERNATIONAL ENTITIES WITH RELEVANT EXPERTISE

The answers to question number one in the attached document (GT/REMJA/doc.47/99) identify national entities with relevant expertise. In addition, the group of experts has identified the following international entities with expertise regarding cyber crime: the Council of Europe, the Group of Eight, the European Union, the Organization for Economic Cooperation and Development, the United Nations (including the Asia and Far East Institute for the Prevention of Crime and the Treatment of Offenders - UNAFEI), and Interpol. Finally, various academic and private sector entities have critical expertise, including telecommunications companies and "incident response teams" such as the Computer Emergency Response Team at Carnegie-Mellon University in the United States.

V. IDENTIFICATION OF MECHANISMS OF COOPERATION WITHIN THE INTER-AMERICAN SYSTEM

A number of existing arrangements can be used to facilitate cooperation against cyber crime, including bilateral and multilateral mutual legal assistance treaties, Interpol, letters rogatory, and informal cooperation mechanisms. In addition, a few countries in the Americas have joined or are in the process of joining the 24-Hour/7-Day a Week Point of Contact Group.

VI. RECOMMENDATIONS

Within the framework of the provisions contained in resolution AG/RES. 1615 (XXIX-O/99) and recognizing the global threat posed by cyber crime and the need for a rapid and appropriate response by the competent national authorities, the Meeting of Experts recommends that the following recommendations be presented, through the Permanent Council, to the Third Meeting of Ministers of Justice or of Ministers or Attorneys General of the Americas:

That states be urged to identify one or more agencies within their country that will have primary authority and responsibility to investigate and prosecute cyber crime.

That states still lacking legislation covering cyber crime take steps to fill that gap.

That member states be requested to make every effort to harmonize their laws on cyber crime in such a way as to facilitate international cooperation in preventing and combating these illicit activities.

That member states determine their training needs in the area of cyber crime and explore bilateral, regional, and multilateral cooperation mechanisms to meet those needs.

That an effort be made to draw up general guidelines to be used in devising legislation covering cyber crimes.

That consideration be given to various measures, including setting up a Voluntary Specific Fund, to support efforts to expand cooperation on this matter in the Hemisphere.

That member states be encouraged to exchange information on cyber crime.

That support be given to dissemination of information regarding OAS activities in this field, including its Web page on the subject.

That states consider the possibility of becoming members of the 24-Hour/7-Day a Week Point of Contact Group, or participating in other existing mechanisms for cooperation or the exchange of information in order to initiate or receive information.

That member states take steps to heighten awareness of this issue among the general public, including users in the education system, the legal system, and the justice system regarding the need to prevent and combat cyber crime.

VII. CONCLUSIONS

In conclusion, the Meeting of Government Experts on Cyber Crime, held under the auspices of the Special Group on Justice of the Permanent Council takes it upon itself to transmit this report to that body. The report summarizes the activities carried out during the meeting of experts and makes recommendations to be submitted for consideration by the Third Meeting of Ministers of Justice or Ministers or Attorneys General of the Americas.

[1]. The list of participants at the Meeting of Experts has been published as document GE/REMJA/doc. /99.