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.15/99 corr. 1
1 June 1999
Original: English

QUESTIONNAIRE PREPARED AT THE FIRST MEETING OF GOVERNMENT EXPERTS ON CYBER CRIME

(Approved at its meeting of May 12, 1999)

QUESTIONNAIRE PREPARED AT
THE FIRST MEETING OF GOVERNMENT EXPERTS
ON CYBER CRIME

1. What investigative, prosecutive, or other entities in your nation have expertise regarding cyber crime (criminal activity which targets computers and information, or which uses computers as the means of committing an offense)?

2. Has your nation experienced any or a significant amount of cyber crime, such as:

    1. the use of computers by criminals to store information relevant to the commission of an offense?
    2. the use of computers by criminals as a means to communicate with other criminals, victims, or other persons?
    3. criminal activity where the use of a computer is a significant part of committing the offense?
    4. criminal activity which targets computers and electronic information, such as unauthorized access to computer systems?

3. Have you ever sought or received a request for international legal assistance in a cyber crime case? What mechanisms were used to provide assistance and how quickly was assistance provided?

4. Does your criminal law define a computer system? If so, please provide the definition and the reference to the related paragraphs/articles of your code.

5. Does your criminal law define computer data? Does this definition include programs or similar coding? If you have a definition, please provide it and the reference to the related paragraphs/articles of your code.

6. Does your criminal law penalize the unauthorized destruction, modification, alteration, access, usage, or other similar interference to or of a computer system or program?

7. Does your criminal law penalize the unauthorized erasure, alteration, rendering inaccessible, acquisition, or other similar interference to or of information or data from a computer system or program?

8. Does your criminal law penalize the unauthorized interception of the transmission in any manner or mode of computer data or information?

9. Is specific intent required in relation to the offenses described in questions 6, 7, and 8?

10. Are the offenses described in questions 6, 7, and 8 indictable?

11. Are the offenses described in questions 6, 7, and 8 extraditable?

12. Would your country have jurisdiction over conduct which amounts to a computer crime as described in the questions above,

    a) if committed solely within your territory,
    if one or more of the constituent elements occurred inside your national territory, and
    if the crime caused damage in your territory?

13. The law of some countries may only permit the seizure of tangible material by investigating authorities. Does the law of your country permit the seizure of intangible computer data (e.g., by printing out or copying the data on to paper or a diskette, which is subsequently seized), or must the physical medium upon which the data is stored (e.g., a computer diskette or the computer itself) be seized?

14. Does your law permit an on-line search of domestic computer systems? If yes, for what types of crimes?

15. Can a telecommunications company or an Internet service provider voluntarily provide data relating to the use of telephone or computer services (e.g., billing or other records of usage, or subscriber identity data) to investigating authorities?

16. Does your country's law permit compelling telecommunications companies or Internet service providers to produce the information referenced in question 15?

17. Does your country's law obligate a) a suspect or b) a third person to provide access (including the giving of passwords) to a computer system or data that is the target of a lawful search?

18. As computer systems may contain large amounts of data, does your country's law permit investigating authorities who are undertaking a search of a computer system to seize:

    a) data that is relevant to the investigation but which is not specified within the scope of the judicial or other order that authorizes the search,
    data that is relevant a crime different from that which is under investigation and specified in the judicial or other order that authorizes the search, and
    without a judicial or other order, data when there is a risk of erasure or destruction of the data?

19. In question 18, can the investigating authorities seize such data without obtaining another judicial order?

20. Does the law of your country permit investigating authorities to search to collect or intercept (or to otherwise obtain) from a) a telecommunications system or b) a computer system, data about the source or destination of a telephone or computer communication at a time that is simultaneous to its time of creation in the present or in the future?

21. Does your law permit the interception by investigating authorities of telephone or computer communications for the purpose of obtaining their informational content?

22. Does the law provide a legal authority or obligation for telecommunications companies or

Internet service providers to undertake or assist in the interception or obtaining of data referred to questions 20 and 21?

23. Does the law allow a telecommunications company or an Internet service provider to monitor the content of communications? If so, can those communications voluntarily be provided to investigating authorities?

24. Does the law obligate telecommunications companies or Internet service providers to preserve data related to a subscriber's identity and data related to communication transactions (e.g., date, time, telephone number, or the Internet address that was contacted)?

25. Can investigating authorities compel a telecommunications company or Internet service provider to preserve data related to a subscriber's identity and data related to communication transactions (e.g., date, time, telephone number, or the Internet address that was contacted) if that data was previously collected by that company or provider?

26. Are statistics kept of the number of computer crime cases

    a) reported by victims?
    b) reported to the police?
    c) tried before court?

27. Does your country offer computer crime training programs to

    a) the police?
    b) the prosecution service?
    c) the judiciary?

28. List mechanisms for technical cooperation in the area of cyber crime.

29. Which measures have been taken with regard to the revision of inter-American instruments for legal and judicial cooperation?