Web site: www.coe.int/economiccrime

COUNCIL OF EUROPE CONSEIL DE L'EUROPE

Strasbourg, 20 March 2006

T-CY (2006) 07
English only

THE CYBERCRIME CONVENTION COMMITTEE (T-CY)

REPLIES TO

THE REQUEST FOR FURTHER INFORMATION T-CY (2006) 02

United States of America

Question 1 Party to the Convention

If your State is a Party to the Convention on Cybercrime, please indicate the steps which were taken (eg amendment of laws) to enable it to become a Party and any experience it has concerning the implementation of the Convention.

If your State is not a Party to the Convention, please indicate any progress which has been made with a view to becoming a Party or any problems preventing your State from becoming a Party.

Response
The United States is not yet a Party to the Convention, but has nearly completed the internal processes necessary for it to become a Party.

After signing the Convention, the United States undertook a careful examination of the Convention and of United States law to determine what, if any, legislation and/or reservations would be required for the United States to become a Party. The result of that examination was a report, sent by the President to the United States Senate on November 17, 2003, outlining the provisions and benefits of the Convention and stating that, with several recommended reservations and declarations, the United States is able to comply with the Convention without further legislation. In that report, the President recommended that the Senate give its advice and consent to United States ratification of the Convention.

In turn, the United States Senate, per its standard practice, referred the Convention and the President's report to its Committee on Foreign Relations. That Committee held a public hearing and collected testimony and written comments on the Convention. After further study, the Committee voted unanimously to recommend that the Senate give its advice and consent to ratification of the Convention. The Committee issued a report containing its recommendation on November 8, 2005.
The Senate subsequently placed the Convention on its "Executive Calendar." This means that the Convention is ready for consideration by the full Senate at a time of its choosing. The final step before the President can ratify the Convention is for the Senate to vote to give its advice and consent to that action.

The United States is aware of no obstacles that would prevent it from becoming a Party.

Question 2

Please give any information you may have concerning any of the following matters:
(a) Any internationally significant legal, policy, or technical developments in the field of cybercrime such as:
i. increasing areas of cybercrime
ii. your experience of the 24/7 network
iii. problems hindering international cooperation
iv. effective means to deal with cybercrime and assist victims

v. steps taken to strengthen cooperation between the public and private sector and promote public and private partnerships
vi. any assistance or training available to other States to assist them to amend their legislation (eg by using the Convention as a model law) or to train their law enforcement officials.
(b) any problems with specific Articles of the Convention and any proposals to extend or amend the Convention

Response:
(a) i. Increasingly, cybercrimes have been linked to online activity for profit. This includes cybercrimes related to identity theft per se, such as phishing and pharming, and the increasing growth of large international rings that market false identity information online. Also, we have noted a rise in the use of botnets (multiple hijacked computers) that have been used to direct denial of service attacks on commercial websites and to accumulate false charges for online advertisements. We have also seen a rise in hacking attacks on large databases storing sensitive personal information.
ii. With the increasing number of participants in the 24/7 network, we have seen a rise in the number of calls, and greater use by participating nations. The United States continues to encourage greater participation by other nations, such as some countries of the OAS, that are not currently participating in the network.
iii. We continue to have problems in obtaining electronic evidence or law enforcement cooperation from nations that have not adequately criminalized online conduct, established means to preserve electronic evidence in a timely manner, or entered into bilateral or multilateral agreements to ensure adequate cooperation in conducting international computer crime investigations. Each of these problems would be addressed by greater international adoption of the Convention.
iv. The Attorney General of the United States has recently issued improved guidance on providing aid and assistance to victims and witnesses in criminal cases. Furthermore, many U.S. states have passed legislation mandating that victims of corporate and government database breaches be given timely notice of any compromise in the security of these databases. At the federal level, there are additional civil remedies available to victims.
v. Increasing, intensive, and by now long-standing outreach by government organizations to private corporations has reduced misunderstanding and has resulted in greater government/industry cooperation in cybercrime investigations. For example, major computer and internet companies have assisted the United States in providing cybercrime training to other nations. Some U.S. internet service providers (ISPs) have developed specific guidance for U.S. law enforcement on how to work with ISPs to obtain evidence in criminal cases. Furthermore, as part of database breach legislation, some U.S. states have mandated the report of such breaches to law enforcement. Also, the U.S. just completed a cybercrime exercise called Operation Cyber Storm. The purpose of the exercise was to test international, federal, state, local, and private cooperation and response to a series of simulated cyber criminal incidents.

vi. The United States makes available to other countries a great number of programs both to assist states in amending their legislation to meet Convention standards and to train law enforcement officials, including investigators, prosecutors, and judges, in cybercrime-related issues. These programs are offered to other countries by the Computer Crime and Intellectual Property Section of the Criminal Division of the Department of Justice; 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 others. To describe them in more detail, the United States will submit a separate paper, and information about such programs may be obtained from the U.S. delegation. An example of such a program is the following. Working through the Organization of American States, and with the assistance of other countries, the United States developed a series of four regional week-long training courses to assist OAS member states in drafting legislation and procedures to allow these states to adopt the Convention. The OAS has now agreed to expand this training by sponsoring additional training, which the United States will develop, on how to establish 24/7 capability and how to develop a computer forensic capability.

(b) The United States does not have any problems with specific Articles of the Convention or any proposals to extend or amend the Convention. Furthermore, the United States believes it is too soon to consider any such extensions or amendments. There are several reasons why the United States believes extensions or amendments should not be considered at this time:

* There are too few Parties, and there has been too little experience under the Convention to justify changes. Article 46 of the Convention contemplates that the Parties, after developing experience under the Convention, would consult to identify any problems that have hindered implementation. This role is left to the Parties precisely because it is only the Parties who can know whether gaps exist, or whether there are problems that inhibit cooperation. The Committee should await a time when the Convention has been more fully tested, and Parties can relate actual experiences under the Convention, rather than attempting to identify potential or hypothetical problems.
* Implementation of the Convention is the most crucial task for Parties and non-Parties alike. In many countries, expertise in cybercrime is limited to a small number of people. The Committee should be focused on supporting those people and countries in their task of implementing the Convention. A new negotiation of an extension or amendment to the Convention would distract from implementation, and may paradoxically undermine the Convention itself. Indeed, if the Convention is not implemented, any extensions or amendments would be ineffective in any event.
* Ratification of the Convention has taken significant amounts of time in some countries, in part because the topic is new and laws must be

amended or adopted. If the Committee begins work on further extensions or amendments of the Convention, that could raise questions that would undermine progress towards ratification.