

AG/RES. 1939 (XXXIII-O/03)

**DEVELOPMENT OF AN INTER-AMERICAN STRATEGY
TO COMBAT THREATS TO CYBERSECURITY**

(Resolution adopted at the fourth plenary session,
held on June 10, 2003)

THE GENERAL ASSEMBLY,

HAVING SEEN the Annual Report of the Permanent Council to the General Assembly (AG/doc.4156/03 add. 4), in particular the section on the matters entrusted to the Committee on Hemispheric Security;

NOTING that the Committee on Hemispheric Security of the Permanent Council, at its meeting on December 3, 2002, addressed the security of critical information systems and considered the need for member states to develop a strategy to address threats to cybersecurity; and

CONSIDERING:

That the United Nations General Assembly, in December 2002, adopted resolution 57/239 concerning Principles for the Creation of a Global Culture of Cybersecurity for Information Systems and Networks;

That at its XII Meeting, the Permanent Executive Committee of the Inter-American Telecommunications Commission (COM/CITEL) pointed out that “building a culture of cyber security to protect telecommunication infrastructures by raising awareness among all participants in the Americas in information systems and networks concerning the risk to those systems and by developing necessary measures to address security risks to respond quickly to cyber incidents” is within CITEL’s mandates;

That the Inter-American Committee against Terrorism (CICTE), at its third regular session, adopted the Declaration of San Salvador (CICTE/DEC. 1/03 rev. 2 corr. 1), in which it recognized threats to cybersecurity as emerging terrorist threats, and, in its Recommendations to the Special Conference on Security (CICTE/doc.6/03 rev. 2), called on member states to strengthen cooperation, to identify emerging terrorist threats, whatever their origin, such as international terrorist activities and threats to cybersecurity, and to adopt measures that raise awareness about those threats, including seminars, training, sharing of experiences, and strengthening of cooperation;

That the Final Report of the Fourth Meeting of Ministers of Justice or of Ministers or Attorneys General of the Americas (REMJA-IV), held in Trinidad and Tobago, recommended that the Group of Governmental Experts be reconvened for the purpose of following up on implementation of the recommendations and mandates provided by REMJA-III and REMJA-IV related to cyber-crime and including consideration of preparing pertinent inter-American legal instruments and model legislation to strengthen hemispheric cooperation in combating cyber-crime; and

That the offer made by Argentina during the third regular session of CICTE to host a cybersecurity conference/workshop in Buenos Aires in July 2003 is intended to address all aspects of cybersecurity and to foster coordination among the various OAS organs, agencies, and entities responsible for the same, and that member states are encouraged to attend with delegations of appropriate level and composition,

RESOLVES:

1. To direct that the Inter-American Committee against Terrorism (CICTE), the Inter-American Telecommunication Commission (CITEL), and the Group of Governmental Experts on Cyber-Crime of the Meeting of Ministers of Justice or of Ministers or Attorneys General of the Americas (REMJA) ensure that the Organization of American States cybersecurity conference, proposed by Argentina, begin work on the development of a draft integral OAS cybersecurity strategy that addresses the multidimensional and multidisciplinary aspect of cybersecurity, and that they report on the results of the meeting, along with any follow-up work deemed appropriate, to the Committee on Hemispheric Security for its consideration.

2. To instruct the Permanent Council to request its Committee on Hemispheric Security to develop a draft cybersecurity strategy for member states, in coordination and collaboration with CITEL, CICTE, the Group of Governmental Experts on Cyber-Crime of REMJA, and any other bodies of the OAS that it may deem appropriate, with deference to their respective mandates, missions, and existing reporting requirements, taking into consideration any relevant activity in member states related to the protection of critical infrastructure, and to present this draft cybersecurity strategy to the Council for its consideration.

3. To request the Permanent Council to report to the General Assembly at its thirty-fourth regular session on the implementation of this resolution.