OAS | CICTE

List of Consolidated Cooperation and Confidence-Building Measures in Cyberspace

1. Provide information on cybersecurity policies, such as national strategies, white papers, legal frameworks, and other relevant documents.

2. Nominate a national point of contact at the policy level able to discuss the implications of hemispheric cyber threats. These points of contact will be distinct from, yet supplement the ongoing work of law enforcement and other technical experts in combating cybercrime and responding to cyber incidents of concern. This information will be updated annually, or as frequently as needed, and shared among partners in a transparent and readily accessible format.

3. Designate points of contact, if they do not currently exist, in the Ministries of Foreign Affairs with the purpose of facilitating work for cooperation and international dialogues on cybersecurity and cyberspace.

4. Develop and strengthen capacity building through activities such as seminars, conferences, and workshops, for public and private officials in cyber diplomacy, among others.

5. Encourage the incorporation of cybersecurity and cyberspace issues in basic training courses and training for diplomats and officials at the Ministries of Foreign Affairs and other government agencies.

6. Foster cooperation and exchange of best practices in cyber diplomacy, cybersecurity and cyberspace, through the establishment of working groups, other dialogue mechanisms and the signing of agreements between and among States.

7. Encourage and promote the inclusion, leadership, and effective and meaningful participation of women in decision-making processes linked to information and communication technologies by promoting specific actions at the national and international levels, with the aim of addressing dimensions around gender equality, and the reduction of the gender digital divide, in line with the women, peace, and security agenda.

8. Promote study, discussion, development, and capacity-building at the national and international levels regarding the application of international law to the use of information and communications technologies in the context of international security by promoting voluntary exchanges of positions and national vision statements, opinions, legislation, policies, and practices on the subject, in order to promote common understandings.

9. Promote the implementation of the 11 voluntary, non-binding norms on responsible State behavior in cyberspace adopted by resolution 70/237 of the General Assembly of the United Nations and promote reporting on these efforts taking into account the national implementation survey.

10. In the sphere of information and communication technologies, promote work and dialogue with all stakeholders, including civil society, academia, the private sector, and the technical community, among others.

11. Develop national cyber incident severity schemas and share information about them.