DRAFT REGIONAL CONFIDENCE-BUILDING MEASURES (CBMs)
TO PROMOTE COOPERATION AND TRUST IN CYBERSPACE

(Agreed during the second meeting of the Working Group on Cooperation and Confidence-Building Measures in Cyberspace on April 24, 2019)

DRAFT PRIORITY MEASURES

Confidence-building measures in cyberspace to promote and strengthen cyber diplomacy

An important challenge in our region is the engagement of the Ministries of Foreign Affairs (MFAs) in cybersecurity and cyberspace policies. There is still a perception that those subjects are more “technical issues” and not necessarily political ones, so the role of MFAs would be secondary or in some cases irrelevant. However, MFAs are essential when generating cooperation between States. MFAs usually coordinate national policies and decisions on cyberspace and cybersecurity towards the international scene.

MFAs and diplomacy are powerful and important tools when it comes to generating not just “cooperation bridges”, but also discussion, work and negotiations on international norms and CBMs, among others. Cyber diplomacy, then, is a crucial dimension for the international discussion of cybersecurity and cyberspace.

Considering that the current process of discussion, negotiation and adoption of CBMs within the framework of the OAS is a good example of the foregoing, it seems logical that States can adopt measures that allow and help strengthen cyber diplomacy.

As a result of the second meeting of the Working Group, Member States agree to the following additional voluntary cyber CBMs to promote and strengthen the engagement of MFAs and diplomacy on cybersecurity and cyberspace policies in our region:

1. To designate points of contact, in the event that none exist, within the Ministries of Foreign Affairs, with the purpose of facilitating the work on international cooperation and dialogue in cybersecurity and cyberspace.

2. Develop and strengthen capacity-building through activities such as seminars, conferences, workshops, among others, for public and private sector officials in cyber diplomacy.
3. To foster the inclusion of cybersecurity and cyberspace subjects into training courses for diplomats and officials of the Ministries of Foreign Affairs and other government agencies.

4. To foster cooperation and exchange of best practices on cyber diplomacy, cybersecurity and cyberspace, through, for example, the establishment of working groups, other dialogue mechanisms, and the signing of agreements among states.

**RECOMMENDATIONS TO IMPLEMENT THE SECOND VOLUNTARY CYBER CBM**

**Purpose of the Second Voluntary Cyber CBM (CBM #2)**

CBM #2 is critical in that identifying appropriate policy points of contact (POCs) allows for participating Member States to work together to quickly respond to concerns regarding cyber activity emanating from another participating Member State’s territory. Having in place pre-identified policy and technical points of contact facilitates rapid exchanges of information and, as needed, cooperative responses that can help to resolve cyber incidents and prevent unnecessary escalation. To be successful, though, such points of contact should be carefully chosen and supported by counterparts throughout their respective governments.

**Implications of an Inquiry**

In order for this CBM to enhance strategic stability and prevent conflicts, it is critical that participating Member States be willing to voluntarily respond to requests for information when contacted. Given that information and communication technology (ICT) incidents can emanate from, or involve, third countries, there is no presumption that a participating Member State that is being contacted is knowingly involved in an ICT incident. Making an inquiry using CBM #2 POCs does not constitute an accusation that the participating Member State receiving the inquiry carried out the activities in question. At the same time, when a participating Member State makes use of the POC provided under CBM #2, it should be understood that the participating Member State making the inquiry views the incident as a potential national security matter.

**Procedure for Making an Inquiry**

Here are the steps we recommend participating Member States follow to request more information from another participating Member State regarding an ICT incident:

1. Refer to the contact list to find the appropriate POC from the participating Member States from whose territory the cyber activity is emanating.
2. Call or email the relevant POC and provide your name and affiliation.
3. Inform the POC that you are invoking OAS CBM #2 in accordance with paragraph 78 of the OAS General Assembly Resolution AG/RES. 2925 (XLVIII-O/18), and that you are contacting the person in question because they are listed as their participating Member State’s POC.
4. Describe the nature of the incident.
5. Ask for additional information about the incident and provide your contact information. Indicate time sensitivity as appropriate.
Procedure for Responding to an Inquiry

Here are the steps we recommend in order to respond to an inquiry about an incident:

- Option 1: Provide an immediate response to the cyber incident query (if possible).
- Option 2: Inform the POC that you will look into the cyber incident and, follow up with additional information, as possible. Ask for the POC’s contact information. Provide an estimated timeframe for a response, as appropriate.

CBM POCs should engage cyber counterparts within their own government or private sector as necessary to collect information and develop an appropriate response. Governments should also consider standing up a consultative working group, if none exist, to ensure officials know whom to contact in order to generate responses in a timely manner.

DRAFT PROCEDURAL CONSIDERATIONS

As a result of the second meeting of the Working Group, Member States acknowledged the importance of implementing the existing and new proposed cyber CBMs.

Members of the Working Group agreed that this document of recommendations on CBMs developed to promote cooperation and trust in cyberspace be presented as a resolution at the Nineteenth Regular Session of CICTE.

Once adopted by CICTE, the list of CBMs would be transmitted to the Committee on Hemispheric Security for inclusion in the “Consolidated List of Confidence- and Security-Building Measures” as a non-traditional measure.