OAS/CICTE experiences related to the development and implementation of (a) inter-governmental Points of Contacts directories in the area of ICT security, and (b) other confidence building measures relating to ICT security

OEWG Informal Inter-sessional Meetings
Secretariat of the Inter-American Committee against Terrorism (CICTE)
Measures to Promote Cooperation and Trust in Cyberspace

**APRIL 2017**

**Establishment** of a Working Group on Cooperation and Confidence-Building Measures in Cyberspace through resolution CICTE/RES.1.17.

**FEBRUARY - MARCH 2018**

**1st Working Group Meeting**

Presentation by the working group of a draft "Cyber CBMs for the Inter-American System" for consideration.

**JUNE 2018**

CBMs approved by the GA/OAS

- Provide information on cybersecurity policies.
- Designate a national cyber point of contact at the policy level.
Measures to Promote Cooperation and Trust in Cyberspace

**APRIL 2019**

*2nd Working Group Meeting*

*4 Additional CBMs Recommended*

- Designate *points of contact* in the Ministries of Foreign Affairs.
- Develop and *strengthen capacities* through cyber diplomacy.
- Promote the incorporation of cyberspace and cybersecurity *training for diplomats*.
- Foster *cooperation and exchange of best practices* in cyber diplomacy, cybersecurity and cyberspace through the establishment of working groups.

**NOVEMBER 2020**

*Informative Session*

Technical Secretariat provided an update on the *status of implementation* of the *agreed voluntary CBMs* and the update of the *UN GGE and OEWG processes* after COVID-19.

**2021**

*3rd Working Group Meeting*

Under the Chairmanship of Chile

*July 27, 2021* (virtual)-

*progress achieved by the WG was discussed*
### Gender:
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 the dimensions around gender equality, and the reduction of the gender digital divide, in line with the women, peace, and security agenda.

### International law:
To promote the 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.

### Implementation of 11 voluntary, non-binding norms:
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.

### Strengthen work with all stakeholders:
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.

Encourage member states to develop their own **national cyber incident severity schemas** and share information about them.
On-going Technical Support for the Working Group

- Maintenance of the list of PoC for Working Group on Cooperation and Confidence-Building Measures in Cyberspace and Cyber-related Policy and Legislation Repository

- Informal briefings and updates on current issues related to the applicability of international law to cyberspace.

- Development of a web portal to manage the cyber policy points of contacts of the OAS Member States and provide them a repository of policies and legislation related to cybersecurity.

- Communication and organization of formal and informal meetings of the Working Group.

- Development of Reports and presentations on the progress of the working group, including reporting to member states on specific mandates.
Contacts

WORKING GROUP ON COOPERATION AND CONFIDENCE-BUILDING MEASURES IN CYBERSPACE

97
Policy contacts

19
Ministry contacts
Contacts
WORKING GROUP ON COOPERATION AND CONFIDENCE-BUILDING MEASURES IN CYBERSPACE

97 Policy contacts

30 Countries

19 Ministry of Foreign Affairs contacts

Countries
Activated accounts
WORKING GROUP ON COOPERATION AND CONFIDENCE-BUILDING MEASURES IN CYBERSPACE

Features include Email, Group emails, Access to Policies and Legislation, updates on diplomacy courses by country presentation
In the future CBMS FAQ tab you could find information about the most common questions from users.
In the future CBMS Cyber news
This will include information from the WG, UN and other partners around the topic of norms, CBMs and responsible state behaviour.
Courses on international cyber diplomacy, international law in cyberspace and international Internet governance laws and standards for government officials.

**Common issues**

- How does international law apply to the use of ICTs by States?
- How do States interpret international law in the context of cyberspace?
- When does a State bear international responsibility for a malicious cyber operation?

**Since 2017**

- +500 officials trained
- +20 courses held
- 31 Member States’ participation
OAS/CICTE CSIRTAmericas Network

210 Specialists
33 CSIRTs
20 Countries

Argentina
Barbados
Bolivia
Brazil
Chile
Colombia
Costa Rica
Dominican Republic
Ecuador
Guatemala
Guyana
Jamaica
Mexico
Panama
Peru
Paraguay
Suriname
Trinidad and Tobago
United States of America
Uruguay
Challenges and Solutions

**Challenges**

- The CBMs are voluntary – no requirement to comply
- On the technical side of the portal – there needs to be a portal manager who ensures user accounts are created
- Dependent on the infrastructure used – need to ensure security updates don’t affect functionality of the portal
- Frequency or lag in user log ins to the portal
- Funding to expand services within the portal

**Solutions**

- Periodic reminders and facilitation of information on existing implemented measures
- A dedicated technical and policy team member to ensure monitoring of infrastructure and content is up to date
- Develop activities such as ping tests, webinars and national and subregional TTX around the Points of Contacts specifically
- Fundraise to ensure continued operationalization of the portal
Important to note

OAS/CICTE is supportive of the proposal of member states on the development of a global POC directory.

OAS/CICTE takes note and agree on the points raised by MS that regional bodies are 1. not organized the same way globally 2. may not comprise of all countries within the geographical mandates.

OAS/CICTE would like to reiterate however the value and importance of regional points of contact listings given it would:

- reduce the touch points for the UN in coordinating in a geographical region where the regional bodies has representations – allowing the UN to be able to have access to example in our context the OAS list and then focus on those countries not represented.
- reduce duplication as the listing could feed directly into the global PoC directory where it exists and once the required mechanisms are implemented and the UN can then build on this.
- facilitate more frequent updates given frequent resource turnover, the regional footprint and pre-existing mandates at the regional level to maintain such a listing (where it exists).
Thank you!

Merci

Gracias

Obrigado

Kerry-Ann Barrett

Cybersecurity Program
Organization of American States
cybersecurity@oas.org
www.oas.org/es/sms/cicte/prog-ciberseguridad.asp