**INTER-AMERICAN COMMITTEE AGAINST TERRORISM (CICTE)**

THIRD MEETING FOR THE WORKING OAS/Ser.L/X.5

GROUP ON COOPERATION AND CONFIDENCE-BUILDING CICTE/GT/MFCC-22/21

MEASURES IN CYBERSPACE 21 July 2021

July 27, 2021 Original: English

Report on Cooperation and Confidence-Building Measures in Cyberspace

(Presented by the CICTE Secretariat)

Contents

[General Overview of Confidence and Security Building Measures at the OAS - 2 -](#_Toc77699893)

[Traditional measures - 2 -](#_Toc77699894)

[Non-Traditional Measures - 3 -](#_Toc77699895)

[Establishment of the Working Group on Cooperation and Confidence-Building Measures in Cyberspace - 3 -](#_Toc77699896)

[First Meeting of the Working Group on Cooperation and Confidence-Building Measures in Cyberspace - 4 -](#_Toc77699897)

[Adoption of the first two Cyber CBMS at the Forty-Eighth OAS General Assembly - 4 -](#_Toc77699898)

[Implementation of the first two approved Cyber CBMs - 4 -](#_Toc77699899)

[Request for nomination - 4 -](#_Toc77699900)

[Development of the Threat Survey - 5 -](#_Toc77699901)

[Draft Work Plan - 5 -](#_Toc77699902)

[Second Working Group Meeting - 5 -](#_Toc77699903)

[On-going Work of the Technical Secretariat - 6 -](#_Toc77699904)

[Fiftieth Regular Session of the OAS General Assembly – Virtual 2020 - 6 -](#_Toc77699905)

[Informal Briefing on the Working Group on Cooperation and Confidence-Building Measures in Cyberspace – Virtual 2020 - 7 -](#_Toc77699906)

[Development of CBMs Network - 7 -](#_Toc77699907)

[Summary - 8 -](#_Toc77699908)

[Consolidated list - 9 -](#_Toc77699909)

Report on Cooperation and Confidence-Building Measures in Cyberspace

(Presented by the CICTE Secretariat)

## **General Overview of Confidence and Security Building Measures at the OAS**

Confidence Building Measures, or CBMs, are a verified instrument of international politics, which aims to prevent the outbreak of war or an (international) armed conflict by miscalculation or misperception of the risk, and the consequent inappropriate escalation of a crisis situation between States. Furthermore, CBMs in the traditional disarmament and arms control arena were developed in an environment where States mostly held the monopoly of use of force and were in possession of a majority of the weaponry and other military means relevant to international peace and security. As the capabilities and knowledge necessary for conducting significant malicious cyber activities are globally widespread – also outside the governmental sector –, the initial situation for the development of CBMs for cyberspace is very different. More specifically to cyberspace, ‘’… the ultimate end‐state desired of CBMs for cyberspace can be described as:

* a common understanding of acceptable State behavior in cyberspace, and
* a state of cyber stability in international relations.[[1]](#footnote-1)

## **Traditional measures**

The Organization of American States (OAS) launched its efforts to develop CBMs at the First Summit of the Americas in the 1990s, with a special focus on traditional CBMs. In 1991 the Member States, meeting at the 21st regular session of the OAS General Assembly in Santiago, Chile, expressed their resolve to begin a process of consultation on hemispheric security in view of new regional and world realities. Through its resolution AG/RES. 1123 (XXI-O/91), "Cooperation for Security in the Hemisphere," the General Assembly entrusted the Permanent Council with setting up a working group, with the specific mandate of studying and making recommendations on cooperation on the various dimensions of hemispheric security. As a result of the work of the working group, the General Assembly, in 1993, through resolution AG/RES. 1237 (XXIII-O/93), resolved to convene the first meeting of government experts on confidence- and security-building measures in the Hemisphere, which was held in Buenos Aires, Argentina, in March 1994.

In December 1994, the Heads of State and Government of the Hemisphere met at the First Summit of the Americas and declared in the Plan of Action their intention to support “actions to encourage a regional dialogue to promote the strengthening of mutual confidence, preparing the way for a regional conference on confidence-building measures in 1995 …”. By 1995, in the Declaration of Santiago on Confidence and Security Building Measures, member states identified 11 measures to build confidence, dialogue, and the exchange of views on hemispheric security-related matters. The Committee on Hemispheric Security has since regularly updated the “Consolidated List of Confidence and Security Building Measures” (CSBMs), which include, among others, the voluntary exchange of information on organization and structure, the exchange of policy papers, the establishment of national points of contact regarding critical infrastructure protection, the ability to share experience and ideas on transparency and CSBMs with other regional security fora, such as the Organization for Security and Cooperation in Europe (OSCE), the ASEAN Regional Forum (ARF), and the African Union (AU).[[2]](#footnote-2)

## **Non-Traditional Measures**

Non-traditional confidence building measures are typically not associated with military operations. The first non-traditional measure of the Organization of American States was proposed by the Delegation of Ecuador during the VI Forum on CSBMs (held on March 12, 2015). The text adopted by CSH on March 3, 2016 as a non-traditional confidence- and security-building measure (CSBM) is as follows:

*“*Exchange information related to adopting and adapting provisions under domestic laws that govern processes for obtaining data and information, and exchange experiences involving government, service providers, end users and others, regarding prevention, management of, and protection against cyber threats, with a view to sustained mutual cooperation to prevent, address, and investigate criminal activities that threaten security and to ensure an open, interoperable, secure and reliable internet, while respecting obligations and commitments under international law and international human rights law, in particular.”[[3]](#footnote-3)**/**

The Working Group on Cooperation and Confidence-Building Measures in Cyberspace is one group that focuses on non-traditional measures, specifically those related to cyberspace.

## **Establishment of the Working Group on Cooperation and Confidence-Building Measures in Cyberspace**

During the Seventeenth Regular Period of Sessions of CICTE (April 6-7, 2017), Member States agreed to establish the Working Group on Cooperation and Confidence-Building Measures in Cyberspace, approved through resolution [CICTE/RES.1/17](http://scm.oas.org/doc_public/ENGLISH/HIST_17/CICTE01114E07.doc) given the need for increased cooperation, transparency, predictability and stability among States in the use of cyberspace. The decision also stemmed from the recommendations contained in the report of the UN Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (UN GGE), presented at the UN General Assembly in 2010 ([A/65/201](http://www.un.org/ga/search/viewm_doc.asp?symbol=A/65/201)), 2013 ([A/68/98](http://www.un.org/ga/search/viewm_doc.asp?symbol=A/68/98)) and 2015 ([A/70/174](http://www.un.org/ga/search/viewm_doc.asp?symbol=A/70/174)); including the need to promote implementation of said recommendations at the regional level.

## **First Meeting of the Working Group on Cooperation and Confidence-Building Measures in Cyberspace**

The first meeting of the Working Group on Cooperation and Confidence-Building Measures in Cyberspace was held from February 28-March 1, 2018. The group considered and approved two (2) “Cyber CBMs for the Inter-American System,” as well as a plan of action to establish additional measures. The Group also agreed that the CICTE Secretariat would serve as the Technical Secretariat for the Working Group.

Presentations were made by the Organization for Security and Cooperation in Europe (OSCE), who offered insights on how that region developed and implemented CBMs, as well as from different member states regarding cyber threats and the need for a common regional lexicon on cyber terminology. The CICTE Secretariat was asked to survey all member states in order to assess the threat level to critical infrastructure in the region and to report the results at the next WG meeting.

The Working Group further recommended that the approved CBMs be considered during the Eighteenth Regular Session of CICTE, which was held May 3-4, 2018 at OAS Headquarters. Member States subsequently approved resolution [CICTE/RES.1/18](http://www.oas.org/en/sms/cicte/Documents/Sessions/2018/FINAL/RES%201%20Resoluci%C3%B3n%20Medidas%20Regionales%20de%20Fomento%20CICTE01217E.doc), which, among other things, agreed to:

1. Approve the two regional Confidence-Building Measures (CBMs) to Promote Cooperation and Trust in Cyberspace that were agreed upon by the Working Group on Cooperation and Confidence-Building Measures in Cyberspace, and include them in the resolution of the Committee on Hemispheric Security that will be transmitted to the forty-eighth regular session of the General Assembly for their inclusion in the *“*[*Consolidated List of Confidence- and Security-Building Measures*](http://scm.oas.org/doc_public/ENGLISH/HIST_18/CP39857E03.doc)” as non-traditional measures; and
2. To continue the work of the Working Group on Cooperation and Confidence-Building Measures in Cyberspace as a permanent mechanism, and that it continues to meet as needed, in person or by digital means, to discuss new and agreed-upon cyber CBMs.

### **Adoption of the first two Cyber CBMS at the Forty-Eighth OAS General Assembly**

On June 5, 2018, the General Assembly adopted, through paragraph 78 of [AG/RES. 2925 (XLVIII-O/18)](https://www.oas.org/en/sla/dil/docs/AG-RES_2928_XLVIII-O-18.pdf), the recommendations of CICTE and its Working Group on confidence-building measures on cybersecurity, and approved the following two priority voluntary cyber CBMs:

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.

## **Implementation of the first two approved Cyber CBMs**

### **Request for nomination**

On June 14, 2018, the CICTE Secretariat, in its capacity as Technical Secretariat to the Working Group, asked Member States to nominate a national expert with knowledge and experience in cybersecurity issues to participate in the ongoing work of the Cyber CBMs Working Group, including those that would participate in the face-to-face and virtual meetings convened by the Chair and Vice-Chair, among other activities. The Secretariat also developed and distributed a template to support Member State implementation of Cyber CBM#1. The template included fields such as: Name of Policy/Document, Brief Description, Responsible Institutions, Effective Date, and Reference/Link. Member States were asked to voluntarily complete the template.

### ***Development of the Threat Survey***

The Technical Secretariat also developed and distributed a survey to identify common cyber threats in the region, including cyber threats to shared critical infrastructure, in order to inform the next meeting of the Working Group. The survey was open for approximately 4 weeks and closed on December 31, 2018.

### **Draft Work Plan**

As co-chair of the Working Group, the Government of Colombia began drafting a work plan to guide the activities of the WG during the period June –December 2018. Among other activities, the work plan proposed: the identification of a national point of contact, development of an information document to guide an informal meeting of the WG, and the hosting of a virtual meeting among nominated experts in December 2018 to prepare for the second formal meeting of the WG. This work plan was not formally concluded.

## **Second Working Group Meeting**

The Second Meeting of the WG was held from April 23-24, 2019. The meeting was attended by delegations from 21 member states, as well as special guests, permanent observers, and representatives of international organizations, the private sector and civil society. During this meeting, the WG recognized various initiatives in the field of CBMs and norms development and considered proposals from member states for advancing regional efforts.

The meeting included a discussion on how to utilize the Cyber Policy Points of Contact Network, as well as a presentation led by MITRE (a not-for-profit U.S. organization that works in the public interest across federal, state and local governments, as well as industry and academia on topics such as cyber-resilience), on proposed mechanisms to implement existing Cyber CBMs. Member states identified that for this working group the PoC ideally needs policy, technical and diplomacy skills, and further identified the need for representatives of Ministries of Foreign Affairs to be more involved so as to effectively coordinate with other national PoCs. Member states also recognized the need to develop partnerships before an incident occurs, and therefore encouraged regular coordination among the PoCs.

The Technical Secretariat presented the results of the threat survey, which received 91 responses from 12 countries. The most common attacks tools used in the region were identified as Malware, Phishing and Ransomware, and the most vulnerable sectors were identified as Financial and Banking, Telecommunications, Health and Public sectors.

Regarding the status of implementation of the two agreed-upon CBMs, 28 member states had designated one or more national experts and 12 countries had submitted cybersecurity related policies.

The Working Group concluded by recommending adoption of four (4) additional CBMs (which are referred to as 3, 4, 5 and 6)[[4]](#footnote-4) and that they be incorporated into the OAS "New Consolidated List of Confidence-Building Measures" and Security "as non-traditional measures.” It also recommended that the Working Group on Cooperation and Confidence-Building Measures in Cyberspace continue as a permanent mechanism, and that it should meet as necessary, in person or by virtual means, to agree on new and established CBMs.

These recommendations were submitted to the [19th Regular Session of CICTE](http://scm.oas.org/doc_public/ENGLISH/HIST_19/CICTE01295E03.doc) for inclusion into the CSH Omnibus Resolution which was approved by [CICTE/RES. 1/19.](http://scm.oas.org/doc_public/ENGLISH/HIST_19/CICTE01297E03.doc) This was later approved by the 49th Regular Session of the General Assembly- Declarations and Resolutions[[5]](#footnote-5).

## **On-going Work of the Technical Secretariat**

In preparation for the 3rd meeting, originally to be held in December 2019, the Secretariat invited all member states to voluntarily update the:

1. List of Points of Contact for the Working Group on Cooperation and Confidence-Building Measures in Cyberspace;
2. Repository of Cyber-related Policy and Legislation

The Secretariat also requested Member States to designate (if they hadn’t already) points of contact in the Ministries of Foreign Affairs to facilitate cooperation and international dialogue on cybersecurity and cyberspace in furtherance of Cyber CBM#3.

## **Fiftieth Regular Session of the OAS General Assembly – Virtual 2020**

Member States continued to recognize the work of the WG during the 2020 OAS General Assembly and [[6]](#footnote-6), *thanked the Government of Chile, in its capacity as Chair of the Working Group on Cooperation and Confidence-building Measures in Cyberspace, for its offer to host the third meeting of the Group when conditions permit, and to request the CICTE Secretariat's support with organizing informal talks in the meantime, using virtual platforms to advance considerations regarding that Group’s mandates*.

Additionally, through AG/RES. 2950 (L-O/20) member states agreed to [emphasis added]:

*G. Promoting cyber security*

*59. To encourage regional action in response to significant malicious cyber incidents that threaten member states’ national security and our common vision of an open, accessible, interoperable, reliable, and secure Internet.*

***60. To urge member states to implement Cyber confidence building measures identified in the OAS List of Confidence and Security Building measures (CP/CSH-1953/20 rev. 1.)***

## **Informal Briefing on the Working Group on Cooperation and Confidence-Building Measures in Cyberspace – Virtual 2020**

On November 11, 2020, with the approval of the Chair, the Technical Secretariat organized a virtual informal briefing on the status of implementation of the 6 agreed-upon voluntary norms and invited Global Partners Digital to make a presentation on the United Nations GGE and OEWG processes during and post-COVID-19. Member States responded by indicating the need to develop other voluntary CBMs in relation to legislation and applicability of international law in cyberspace, the need to strengthen collaboration at the CSIRT level (taking into account CSIRTsAmericas Network), and also suggested strengthening cross-regional cooperation and information sharing with partners such as OSCE.

Over 50 participants from Member States were brought up to date on progress of implementation of the agreed CBMs, including that: 16 countries have submitted cyber-related policies, 28 countries have submitted cyber-policy points of contact and 8 countries have since updated their points of contact.

## **Development of CBMs Network**

The Technical Secretariat is in the process of developing a web portal to manage the cyber policy points of contacts of the OAS Member States and provide them with a repository of policies and legislation related to cybersecurity. This portal will facilitate transparency among the points of contacts, as well as access to information. Data contained on the portal will be administered by the Technical Secretariat as submitted voluntarily by the Member States. The information contained in the portal could also be used to report on broader CBMs implementation.[[7]](#footnote-7)

It is anticipated that the web portal will be accessible to member states by the 4th Quarter of 2021.

## **Summary [[8]](#footnote-8)**

|  |  |
| --- | --- |
| **Year** | **Measure** |
| 2017 | Establishment of the Working Group on Cooperation and Confidence Building measures in Cyberspace |
| 2018 | Member States agreed to provide information on cybersecurity policies, such as national strategies, white papers, legal frameworks, and other relevant documents |
| 2018 | Member States agreed to 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. |
| 2019 | Member States noted with satisfaction ay the Nineteenth Session of CICTE, the results of the second meeting of the Working Group, held April 23 and 24, 2019 in Santiago, Chile, contained in document CICTE/GT/MFCC/doc.12/19 rev. 2 corr.1 1. To agree to the [four Regional Confidence-Building Measures](http://scm.oas.org/doc_public/ENGLISH/HIST_19/CICTE01284E02.doc) (CBMs) to Promote Cooperation and Trust in Cyberspace, as well as the recommendations to implement the second measure, that were agreed upon by the Working Group on Cooperation and Confidence-Building Measures in Cyberspace during its second meeting, and include them in the resolution of the Committee on Hemispheric Security that will be transmitted to the forty-ninth regular session of the General Assembly for their inclusion in the “Consolidated List of Confidence- and Security-Building Measures” as non-traditional measures.
2. To continue the work of the Working Group on Cooperation and Confidence-Building Measures in Cyberspace as a permanent mechanism, and that it continues to meet as needed, in person or by digital means, to discuss new and agreed-upon cyber CBMs.
3. To consider the possibility of making voluntary contributions, through CICTE’s Cybersecurity Program, to support the work of the Working Group on Cooperation and Confidence-Building Measures in Cyberspace.
4. That the CICTE Secretariat, through its Cybersecurity Program, continue to act as Technical Secretariat for this Working Group and organize its meetings within available financial and human resources.
 |
| 2020 | During the Virtual Fiftieth Regular Session of the OAS General Assembly Member states agreed the following and noted in relation to the CBMs WG [emphasis added]:*G. Promoting cyber security**59. To encourage regional action in response to significant malicious cyber incidents that threaten member states’ national security and our common vision of an open, accessible, interoperable, reliable, and secure Internet.* ***60. To urge member states to implement Cyber confidence building measures identified in the OAS List of Confidence and Security Building measures (CP/CSH-1953/20 rev. 1.)*** |

##

## Consolidated list

[http://scm.oas.org/doc\_public/ENGLISH/HIST\_20/CP41996E07.docx](http://scm.oas.org/doc_public/ENGLISH/HIST_20/CP41996E07.docx%22%20%5Ct%20%22_blank)

CICTE01396E01.docx

1. <https://www.ccdcoe.org/uploads/2018/10/CBMs.pdf> [↑](#footnote-ref-1)
2. CONFIDENCE AND SECURITY BUILDING MEASURES (CSBM) INVENTORY UPDATE REPORT (reported in 2020) <https://drive.google.com/file/d/1IdH95x-aM46-4wPH9RqXjb7yq4j0kcX-/view> and <http://www.oas.org/mfcs/> [↑](#footnote-ref-2)
3. . The Government of the Republic of Nicaragua acknowledges confidence- and security-building measures as a mechanism that helps to foster an international climate of trust and peace in the region. It agrees with the need that such measures be consistent with geographic, political, social, cultural, economic, and technological conditions and realities. In that sense, it is broadly in favor of a confidence-building measure involving the exchange of information related to adopting and adapting provisions under domestic laws that govern processes for obtaining data and information, and exchanges of experience among governments regarding prevention, management of, and protection against cyber threats. Furthermore, the participation of service providers and end-users under this measure should be voluntary and should not entail any obligation for States. [↑](#footnote-ref-3)
4. 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.

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

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.

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. [↑](#footnote-ref-4)
5. AG/RES. 2930 (XLIX-O/19)- International Law And Ag/RES. 2945 (XLIX-O/19) Advancing Hemispheric Security: A Multidimensional Approach(Adopted at the first plenary session, held on June 27, 2019) <http://scm.oas.org/IDMS/Redirectpage.aspx?class=AG/doc.&classNum=5682&lang=e> [↑](#footnote-ref-5)
6. Resolution “Advancing Hemispheric Security: A Multidimensional Approach,” agreed to during the Fiftieth Regular Session of the General Assembly held October 20 and 21, 2020 [↑](#footnote-ref-6)
7. <https://www.jid.org/?page_id=2283&lang=en> [↑](#footnote-ref-7)
8. Overview of Cyber CBMS:

	* Provide information on national cybersecurity policies, such as national strategies, white papers, legal frameworks and other documents that each Member State considers relevant.
	* Identify a national point of contact at the political level to discuss the implications of hemispheric cyber threats.
	* 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.
	* Develop and strengthen capacity building through activities such as seminars, conferences, and workshops, for public and private officials in cyber diplomacy, among others.
	* 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.
	* 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. [↑](#footnote-ref-8)