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

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

GROUP ON COOPERATION AND CONFIDENCE-BUILDING CICTE/GT/MFCC-23/21

MEASURES IN CYBERSPACE 9 August 2021

July 27, 2021 Original: English

THIRD MEETING OF THE WORKING GROUP ON COOPERATION AND

CONFIDENCE-BUILDING MEASURES IN CYBERSPACE

RAPPORTEUR REPORT

July 27, 2021

Excellent and distinguished heads of delegation

Distinguished delegates

Special guests

Ladies and gentlemen:

I would like to start by thanking you for the work and progress made in our first virtual meeting of the Working Group on Cooperation and Confidence-Building Measures in Cyberspace of the Inter-American Committee against Terrorism (CICTE). As Rapporteur of this meeting, the U.S. Delegation is honored to present this report on the interventions made today.

The Third Meeting of The Working Group on Cooperation and Confidence-Building Measures in Cyberspace was held virtually on July 27, 2021. The Third Meeting of the Working Group was attended by 16 delegations from the Organization of American States (OAS) Member States including Argentina, Brazil, Chile, Colombia, Costa Rica, the Dominican Republic, Ecuador, Guatemala, Guyana, Mexico, Nicaragua, Panama, Paraguay, Peru, Trinidad and Tobago and the United States, as well as special guests, permanent observers, and representatives of international organizations.

The meeting began with opening remarks from **Carlos Landeros**, Representative of the Government of Chile and National Director of the national CSIRT of Chile, in Chile’s capacity as Chair of the Working Group on Cooperation and Confidence-Building Measures in Cyberspace. Mr. Landeros noted the global trend of increasingly frequent and destructive cyberattacks with the potential to impact the economies, democratic systems, and societies of Member States. He also noted the multinational scope to cyber risks and the need for practical cooperation in relation to risk management. Mr. Landeros provided a summary of existing cyber confidence-building measures (CBMs) developed and adopted by the Working Group and noted that to the extent they are implemented, they will help consolidate an effective network of support in the Hemisphere. He noted these meetings are meant to promote trust and cooperation. Mr. Landeros also spoke about the importance of promoting gender equity in the field of cyber issues and noted work done under Chile’s administration regarding this issue.

On behalf of the General Secretariat, **Arthur Weintraub**, OAS Secretary for Multidimensional Security, welcomed Member States and thanked them for their participation in today’s meeting. He thanked the Governments of Chile and Mexico for their extraordinary leadership as president and vice president of the Working Group from 2019-2020. Mr. Weintraub noted CBMs are tools to counteract cybercrime and other cyber threats and to promote trust, transparency and diplomacy. This supports the work of United Nations Group of Governmental Experts on Advances in the Field of Information and Telecommunications in the Context of International Security (UNGGE) and the Open-Ended Working Group (OEWG). He noted the Working Group has the capacity to assist Member States in their multilateral activities in this space.

Member States on the videoconference then approved the meeting’s draft agenda, distributed on July 7, 2021, as document CICTE / GT / MFCC-18/21, and the draft schedule, distributed on July 13, 2021, as document CICTE / GT / MFCC-20/21.

**Alison August Treppel**, Executive Secretary of CICTE, spoke about the Portal of the Network of Points of Contact that the CICTE Secretariat is developing, and about the possibility of a practical exercise utilizing the Portal for members of the Network. This work fulfills a request from Member States for the Secretariat to assist with implementation of the group’s first three CBMs.

**Sofia Hunter**, OAS-CICTE Cybersecurity Program Officer, provided a review of the Portal. Ms. Hunter spoke on behalf of the CICTE Secretariat about the objectives of the Portal and illustrated the presentation with a descriptive prototype of the Portal to facilitate the understanding of the format and utilization. The main goal of the Portal is to increase transparency and accessibility for Member States to exchange information, including policy or legal documents as well as Point of Contact information, in line with the Working Group’s CBMs.

**Kerry-Ann Barrett,** CICTE Cybersecurity Program Officer, invited Member States to consider how their governments would respond to a hypothetical cyber incident in the region. Ms. Barrett described a hypothetical cyberattack on a hypothetical regionally important airport and encouraged Member States to consider the questions: How would your agency respond to such an incident? Do you have formal plans for a response? Which agencies do you need to notify, and who do you contact if they’re unavailable? Finally, what could be the role of regional or international organizations? Ms. Barrett noted the usefulness of having a list of Points of Contact available, such as the list to be available under the Portal. She noted that after the Portal launches, the Secretariat plans to hold a call with Member States to verify all the contact information listed there and to request continuous updates from Member States when Points of Contact change. The Secretariat also plans to hold practical exercises utilizing the Portal.

Ms. Barrett then provided a presentation on support the CICTE Secretariat has provided to Member States in the past several years for implementation of existing CBMs. She noted the Secretariat’s mandate from Member States to support them in the implementation of the 11 voluntary, non-binding norms agreed upon by Member States based on a report from the UNGGE. She noted 16 OAS Member States had shared public policies related to cybersecurity, per one of the group’s CBMs, and 28 have submitted Points of Contact (POCs). CICTE’s ongoing technical support for the Working Group includes maintaining the list of POCs submitted by Member States, providing informal briefings and updates on issues related to the applicability of international law in cyberspace, and the development of a Web portal to manage the cyber policy POCs and present a repository of regional policies and legislation related to cybersecurity. The Secretariat aims for the Portal to be online by October 1, 2021. The Secretariat has also developed training courses for officials from government ministries on the applicability of international law in cyberspace.

The floor was then opened for Member States to provide brief interventions on their efforts to implement existing CBMs. Seven countries made interventions, as follows:

* **United States:** The U.S. delegate noted U.S. support for the work of the OAS and CICTE on these issues, particularly this Working Group. She noted the U.S. is pleased to continue providing financial support for the work of the group, the Secretariat, and the development of the Portal. The U.S. delegate shared that the Biden Administration has continued to prioritize cyber as a policy imperative and has issued a new Executive Order on cyber issues. The United States will share this document for the OAS Policy Repository. The U.S. Department of State has provided an internal training for U.S. cyber diplomats posted throughout the region. They believe this will strengthen the network of policy experts prepared to engage on these issues throughout the region and the world. The U.S. pledged to continue engaging regional partners and OAS Member States on key cyber diplomacy topics in 2022.
* **Chile**: The Chilean delegate noted Chile has focused on building a structure to strengthen responses to cyber incidents. Steps include expanding cooperation internationally by building a list of trusted points of contact and conducting information exchange. One way in which information exchange occurs is through the CSIRT Americas network under CICTE. The Chilean delegate also noted Chile’s work domestically on cyber-related legislation, a process that takes much time to complete. One current legislative effort is related to the Budapest Convention on cybercrime. Another relates to critical infrastructure protection, an area that requires cooperation between the public and private sectors. The Chilean delegate also noted the importance of providing assistance on related issues to other Member States.
* **Mexico:**  The Mexican delegate thanked Chile and the Secretariat for holding this meeting despite the difficulties presented by the global response to COVID-19. He further noted the criticality of holding this type of meeting precisely because of the circumstances around that response. The Mexican delegate shared that Mexico has emphasized five elements in its implementation of the regional CBMs.
  + First, Mexico has reasserted the applicability of international law to cyberspace, including with its participation in this Working Group.
  + Second, by participating in recent developments in the UN, Mexico has contributed to the efforts to build and affirm the framework for the actions of responsible state behavior in cyberspace. Mexico is very excited to see that the work of this group, enhancing trust in cyberspace, will also support this effort.
  + The third relevant point is to keep a balance between the importance of safety and security in cyberspace while allowing for the innovation of technology and the promotion of human rights online.
  + The fourth point is to engage other non-governmental stakeholders.
  + The fifth point is to engage within multilateral organizations in the event of an incident.
  + Based on these five principles, Mexico has convened an interagency group to make decisions on incident response and to advance cyber policy. Mexico has also focused on CERT advancement and worked through the process of developing a comprehensive cybersecurity policy at all levels, state and federal. Mexico also created a national cybersecurity week to promote cybersecurity awareness.
  + The Mexican delegate asked how the Portal initiative can avoid duplication of efforts with the UNIDIR cyber policy portal and the new CSIRT Americas Portal. The CICTE Secretariat said they would respond at the end of the session.
* **Argentina:** The Argentinian delegate noted that building trust contributes to international security and stability in cyberspace. He highlighted the positive work of the UN GGE and OEWG, which this year concluded with consensus reports supporting the framework for responsible state behavior. Argentina, with others in region, promotes establishment of joint action programming within the OEWG. Argentina emphasized the importance of sharing information for the stability of cyberspace, as well as the importance of regional organizations. Argentina stated that it supports all CBMs and has implemented all six measures.  The country created the National Cybersecurity Committee, which contributes to the elaboration of the National Cybersecurity Strategy, currently under revision. Furthermore, the country is developing a program on the protection of critical infrastructure. Additionally, Argentina considers gender perspective in cybersecurity as a priority and aims to foster the increased participation of women in the sector. Furthermore, Argentina has a National CSIRT for the coordination and management of incidents at the national level, and it is also a member of CSIRTAmericas. Finally, the country organizes capacity building programs and courses for their diplomats and policymakers. Argentina believes the Portal and practical exercises will be important. Argentina also noted the threat of cybercrime is a top priority for cooperation among Member States, and that Argentina is a signatory to the Budapest Convention on cybercrime.

* **Colombia:** The Colombian delegate said Colombia has been participating in the OEWG, which Colombia views as its own measure to promote trust. She mentioned two milestones regarding the implementation of CBMs in cyberspace. First, Colombia ratified the Budapest Convention on cybercrime and is working on its implementation. Second, the country created a new policy, CONPES 3995, which is the third cybersecurity public policy and helps the country identify national priorities. Colombia is looking at all levels regarding training. Colombia would like to see guidelines from the OAS regarding the applicability of international law to assist Member States in their implementation.
* **Dominican Republic**: The Dominican representative said the Dominican Republic has had a cybersecurity strategy since 2018 and has sought to advance interaction among various sectors to promote trust. The Dominican Republic’s national cybersecurity council includes institutions working on transformation of government policies, telecommunications, public prosecution, and justice. The Dominican Republic is working to update its 2007 law regarding cybercrime and recently finished a draft law that may complete the legislative process this year. The government also worked with the private sector to design a law that would cover the entire digital ecosystem in the Dominican Republic, emphasizing critical infrastructure. The Dominican Republic is also moving forward with a law to protect data. The Dominican Republic has a workplan to draft sectoral regulations for each critical infrastructure sector and plans to do a risk analysis in 2022 to create an official catalog of national critical infrastructure. A previous analysis by the Dominican Republic found multiple cyber incidents were related, raising concerns. To strengthen operational capacity on incident response beyond its national CSIRT, the Dominican Republic is establishing sectoral CSIRTs as well. The finance sectoral CSIRT is well established, there is a nascent CSIRT for the defense sector, and an energy sector CSIRT may follow next year. The Dominican Republic has a digital agenda for the coming decade related to legislation and digital transformation, with cybersecurity as a cross-cutting issue. The Dominican Republic will produce an updated cybersecurity strategy in about three years. The national CIRST of the Dominican Republic, the CSIRT for the financial sector, and other CSIRTs are members of CSIRTAmericas. The Dominican delegate noted the country’s selection by the European Union Cybernet project to host a regional center for capacity building on cybersecurity and combating cybercrime. The Dominican Republic plans to have specialized training facilities open to all countries in Latin America and the Caribbean.
* **Ecuador**: The Ecuadorian delegate said Ecuador has recently had a change in administration and is working to maintain cybersecurity as a focus. Among the actions taken by the Ecuadorian Government to implement cybersecurity CBMs, the country created a National Committee of Cybersecurity. Furthermore, Ecuador approved a new law regarding data protection and is currently aiming to follow the Budapest Convention and improve national capacity building efforts.
* The discussion concluded with the CICTE Secretariat responding to the questions posed by the delegate of Mexico. CICTE Secretariat, as the Technical Secretariat, makes an extensive effort to avoid duplication of effort and to coordinate with other entities. UNIDIR and OSCE both have portals and the Secretariat has not yet planned any joint efforts. The Secretariat is focused on serving Member States and is open to joint initiatives in the future. The CICTE Secretariat is managing both the technical and policy portals that are being created, which will allow the Secretariat to identify practical measures that could facilitate cooperation and collaboration between those two groups.

The next segment was dedicated to open discussion among Member States on lessons learned and ongoing challenges regarding implementation of cyber CBMs adopted by the Working Group. Two countries made interventions, as follows:

* **United States**: The U.S. delegate shared reflections on challenges in the processes of formulating and implementing cyber policy. To facilitate coordinating across multiple government agencies, the U.S. found it helpful to have both formal and informal mechanisms for cyber coordination in place before an incident occurs. It also is important to have the strengths, authorities, or mandates of any particular agency outlined in policies in advance. It is also important for cyber policy and legislation to be as technologically neutral as possible, to avoid technological change making such documents lose relevance over time. Another challenge is scarce resources and the need to balance between short- and long-term needs. The U.S. Department of State appointed an officer responsible for cyber issues at each of its Embassies abroad, to ensure each Embassy has an officer trained on cyber issues and who can manage cyber diplomatic interactions.
* **Colombia:** Two delegates from Colombia provided interventions. Colombia proposed a meeting at the ministerial level under the umbrella of the OAS, where the topic of cyber diplomacy could be fostered, aiming to increase cybersecurity awareness and engagement, thereby aligning to the current efforts to implement CBMs. At each Embassy, Colombia has Ministry of Defense attaches who act as the points of contact for various institutions.

Secretary Alison Treppel reiterated the disposition of the CICTE Secretariat to support the implementation process of CBMs and expressed the gratitude of the Secretariat to its various donors.

No Member States submitted any proposals from for new CBMs in cyberspace.  The Secretariat invited Member States to submit later proposals in writing.

The following part of the meeting included three presentations, as follows.

**Duncan Hollis**, Laura H. Carnell Professor of Law at Temple Law School, said in his presentation that states agree international law applies to state cyber operations, but there is still little knowledge about the specific way in which international law applies, mainly because most states remain silent on this topic. He offered a conceptualization of the terms of “use of force,” "state responsibility," and "attack" under International Humanitarian Law (IHL). The presentation concluded with the challenges to further transparency on IHL application in cyberspace and potential actions for the future.

**Dan McBryde**, Senior Policy Advisor for Global Affairs Canada, provided a presentation summarizing the evolution and progress of the Group of Government Experts and the Open-Ended Working Group since 2015. He described differences between the two mechanisms and concluded by describing potential future actions. He described the 11 norms of responsible state behavior in cyberspace, adopted by the 2015 GGE, as the foundation on which everything else rests. In Canada’s view, there is no need to create new norms, rather efforts should concentrate on implementing the existing ones.  Mr. McBryde said Canada hopes to issue a statement by the end of 2022 on how the Canadian government believes international law applies in cyberspace.

**Isaac Morales**, Coordinator for Multidimensional Security in the Ministry of Foreign Affairs of Mexico,spoke about the proposal from Mexico and other countries for a National Survey of Implementation of UN General Assembly Resolution 70/237.This voluntary initiative would contribute to the implementation of policies, the identification of challenges, and the coordination of technical assistance for different countries. Mr. Morales offered that Mexico can answer any questions about the survey initiative from Member States, and he invited all Member States to participate in the initiative. Mr. Morales emphasized the importance of multilateral consultation and regional organizations in ensuring safety in cyberspace.

Secretary Alison Treppel thanked the three speakers for their presentations and confirmed that the materials shared during the presentations will be sent to the Member States. She then closed the part of the meeting moderated by the CICTE Secretariat, giving the floor back to Chile.

Member States then discussed the date and location for the fourth meeting of the Working Group on Cooperation and Trust-Building Measures in Cyberspace. Delegates made the following remarks:

* Chile proposed holding the next meeting during the first semester of 2022 in person in Chile, if conditions permit.
* The United States supported Chile's proposal of having a face-to-face meeting in 2022, if conditions allow.
* Colombia accepted Chile's proposal and proposed a hybrid format for the meeting to allow participants to join either online or in person.
* Mexico emphasized the importance of flexibility regarding the format of future meetings.
* Costa Rica supported the need for flexibility both on the dates and modality of the next meeting.

The Chancellery of Chile then presented draft language to be considered for inclusion in the omnibus resolution and opened the floor for interventions by the Member States.

* Colombia proposed eliminating the third paragraph. Furthermore, it highlighted the importance of holding the following meeting in a flexible and hybrid manner.
* Mexico highlighted the need to write acronyms such as “GGE” in English or to add their full names to avoid confusion.
* The United States suggested dividing the fourth paragraph into two parts, highlighting the idea that the Working Group agreed to meet again.
* Colombia expressed concern about the word "articuladas" (“articulated”) and proposed replacing it with "contenidas" (“contained”).
* Mexico referred to the U.S. proposal, arguing that dividing the fourth paragraph into two sections would imply repeating a section mentioned in another paragraph. Given the importance of maintaining a reduced number of paragraphs, Mexico proposed maintaining Chile's proposal adding the modifications requested by the United States.
* The United States agreed to maintain the four paragraphs and proposed further discussion during the CICTE meeting.

The meeting then proceeded to the election of authorities and the floor was opened for nominations.

Canada and Argentina nominated Mexico for the office of the Presidency. Mr. Landeros thanked them for presenting the candidacy and congratulated the delegation of Mexico for their election by acclamation. He expressed gratitude to Mexico for accepting this important mission and offering to lead regional efforts to improve cooperation, transparency, predictability, and stability and reduce the risks of misinterpretation, escalation, and conflict that may arise from the use of ICTs.

Mexico expressed its gratitude to all the delegations for the Presidency of the Working Group and highlighted that it would continue to work on the foundation built by Chile and foster cooperation within the Working Group.

Chile nominated the United States for the office of the Vice-Presidency. Mr. Landeros took the opportunity to congratulate the delegation of United States for their election by acclamation.

Mr. Landeros gave the floor to the United States to present the Rapporteur’s report for consideration and approval. The United States presented an overview of the interventions made during the meeting and noted a formal report would be shared soon.

There being no further requests to speak, Mr. Landeros thanked the delegations for their comments and declared closed the Third meeting of the Working Group on Measures to Promote Cooperation and Trust in Cyberspace.

CICTE01414E01.docx