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

FIFTH MEETING OF THE WORKING GROUP OAS/Ser.L/X.5

ON COOPERATION AND CONFIDENCE-BUILDING CICTE/GT/MFCC/doc.14/24

MEASURES IN CYBERSPACE 18 April 2024

February 26-27, 2024 Original: English

Washington DC, United States

REPORT OF THE FIFTH MEETING OF THE WORKING GROUP ON COOPERATION AND CONFIDENCE-BUILDING MEASURES IN CYBERSPACE

(Prepared by the CICTE Secretariat)

REPORT OF THE FIFTH MEETING OF THE WORKING GROUP ON COOPERATION AND CONFIDENCE-BUILDING MEASURES IN CYBERSPACE

(Prepared by the CICTE Secretariat)

**Introduction**

In accordance with resolution [CP/RES. 1245 (2480/24),](http://scm.oas.org/doc_public/ENGLISH/HIST_24/CP49022E03.docx) the Fifth Meeting of the Working Group on Cooperation and Confidence-Building Measures in Cyberspace (“Fifth CBMs WG Meeting”) was held at OAS Headquarters in Washington DC on February 26-27, 2024. Member States participating in the meeting were as follows: Antigua and Barbuda, Argentina, The Bahamas, Bolivia, Brazil, Canada, Chile, Colombia, Costa Rica, Dominica, Dominican Republic, Ecuador, El Salvador, Grenada, Guyana, Jamaica, Mexico, Panama, Peru, St. Kitts and Nevis, St. Vincent and the Grenadines, Uruguay and the United States of America. All meeting documents are available at: https://www.oas.org/ext/en/main/calendar/event/id/140

<https://www.oas.org/ext/en/main/calendar/event/id/140>

**Opening Session**

The meeting was opened by Jennifer Bachus, Principal Deputy Assistant Secretary, Bureau of Cyberspace and Digital Policy, U.S. Department of State. Ms. Bachus highlighted the contributions of the Working Group in formulating and approving cyber CBMs in the OAS region. The Working Group’s efforts, she noted, furthered the UN framework for ensuring a more secure cyberspace and for promoting peace and security in the region.

Ambassador Claudio Peguero, Advisor on Cyber-Matters of the Ministry of Foreign Affairs, Dominican Republic, and Vice-Chair of the Working Group on Cooperation and Confidence Building Measures in Cyberspace then underscored the importance of CBMs implementation for strengthening cooperation between Member States. He also highlighted the work of the group in establishing a framework for exchanging information, in developing greater capacity, and in adopting practices that promote trust and stability in cyberspace. He emphasized that cybersecurity has become a fundamental challenge that requires a collective and coordinated response.

Ivan C. Marques, Secretary for Multidimensional Security, Organization of American States, also provided opening remarks. He noted that the Working Group supports the UN’s work, particularly the United Nations Groups of Governmental Experts on Development in the Field of Information and Telecommunications in the Context of International Security (UN GGE) and the United Nations Open-ended Working Group on Cybersecurity (OEWG). He reaffirmed the OAS’s ongoing commitment to supporting Member States in implementing the eleven (11) CBMs already agreed upon by the Working Group during its previous four (4) meetings.

**First plenary session**

Liesyl Franz, Deputy Assistant Secretary for International Cyberspace Security, Bureau of Cyberspace and Digital Policy, U.S. Department of State, chaired the Working Group.

During the first plenary session, delegations considered and approved, without modifications, the draft agenda and draft schedule of the meeting.

**Second plenary session**

The Chair began by referring to the five confidence-building measures (CBMs) agreed upon during the fourth meeting of the Working Group, and by welcoming new proposals to enhance the implementation of existing measures. The Chair also referenced the CBMs currently under global discussion, including CBMs on Points of Contact, and encouraged OAS Member States to support UN efforts in this regard.

Kerry-Ann Barrett, Manager of CICTE’s Cybersecurity Program, reported on 2022-2024 activities carried out to implement approved cyber CBMs. Among other things, she informed that currently 89 Cyber Policy Contacts and 19 Ministry of Foreign Affairs Contacts from 30 OAS Member States have access to the internal portal of the Working Group. She also highlighted two recent CICTE initiatives: (1) alignment of CICTE’s cyber diplomacy and international law courses with topics related to approved CBMs and (2) a prototype to improve services of the Working Group Portal.

Mariana Jaramillo, Cybersecurity Program Officer, then presented the 2024 proposed workplan, including activities to update the portal; launch a new webinar series regarding approved CBMs; and continued alignment of CICTE’s existing and new capacity-building initiatives with the approved CBMs. The presentation concluded with the results of the voluntary CBMs implementation survey.

The delegations of Argentina, Bahamas, Canada, Chile, Colombia, Costa Rica, Dominica, Ecuador, El Salvador, Guyana, Mexico, Peru and the United States then took the floor to offer comments and/or thanks to the CICTE Secretariat.

**Third Plenary Session[[1]](#footnote-2)**

Member States then offered updates regarding their cybersecurity policies, recent cyber-related experiences, and lessons learned on cyber-capacity building:

* *Canada* mentioned the recent amendment to its Critical Cyber Systems Protection Act, which establishes a regulatory framework for incident reporting to the government and mechanisms to prevent malicious activity affecting National Critical Infrastructure. Canada has also appointed a cyber digital policy profile and designated a representative to further integrate cyber policy domestically and globally. Canada also referred to the Pall Mall Process sponsored by the Governments of France and United Kingdom, which seeks to address the dangers stemming from the commercial cyber intrusion capability ecosystem, and invited interested delegations to participate in the process.
* *Chile* provided an overview of their recently published National Cybersecurity Policy (2023-2028) and implementation plan, which, among other things, addresses the application of international law in cyberspace, including human rights law; the importance of cyber diplomacy; artificial intelligence; organized crime; gender perspectives and cyber defense-related issues. Chile expressed the need for legal expertise in international law applicability in cyberspace in order to more effectively address cybercrime activities.
* *Colombia* shared that it is currently updating its digital policies, including a new National Cybersecurity Strategy, and is establishing a cybersecurity department. Colombia identified challenges to addressing cyber risks, such as the high cost involved, the evolving nature of threats, and the difficulty of attributing malicious actions. Furthermore, Colombia emphasized the need for cybersecurity capacity building, improving security infrastructure, implementing risk management, and reducing the digital divide, while avoiding duplication of efforts. Colombia highlighted its efforts to deliver cyber diplomacy courses for diplomats.
* The *United States* reported the launch of a new National Cybersecurity Strategy, which calls to rebalance the responsibility for defending cyberspace towards the most capable actors and realigning incentives to favor long-term investments in security. The United States also noted the release of its National Cyber Workforce and Education Strategy and reflected that investments in people, processes, and technology were mutually reinforcing areas of capacity building. The United States expressed openness to collaborating on cyber capacity building and mentioned an upcoming International Cyberspace and Digital Strategy.
* *El Salvador* expressed its goal of becoming a technological hub in the OAS region. El Salvador underscored the progress made in establishing a legal and policy framework to promote cyber capabilities and to address vulnerabilities in national critical infrastructure and information resources, including a National Cybersecurity Strategy. El Salvador also highlighted recent legislation, such as the Innovation and Technological Manufacturing Promotion Law, and a Joint Declaration on Shared Priorities in Digital Policy, issued recently by El Salvador and the United States.
* *Argentina* highlighted its new National Cybersecurity Strategy developed in conjunction with the private sector. The NCS addresses incident response protocols; observance of international standards; and coordination with other multilateral processes.
* *Brazil* highlighted its new National Cybersecurity Strategy and the development of a new legal framework, along with the creation of guidelines and booklets accessible through official ministry websites. Additionally, Brazil is training public servants on these issues and actively participating in various international forums such as BRIC, MERCOSUR, OAS, and OEWG.
* *Costa Rica* reported on the development of its Second National Cybersecurity Strategy, designating cybersecurity as a national priority and aiming to enhance its digital security.
* *Mexico* noted it continues to incorporate international standards on cybersecurity by adapting them to the Mexican context, while emphasizing the need to promote cooperation and dialogue with international partners. Mexico highlighted the growing fragmentation of dialogue and multilateral processes, emphasizing the need for a broader perspective among these fora. Mexico emphasized the importance of standardizing legislative frameworks to build resilience and to protect critical infrastructure and information systems. Mexico noted that developing capabilities has been crucial for overcoming resource constraints.
* The *Dominican Republic* emphasized the importance of implementing approved cyber CBMs. The Dominican Republic outlined the progress made in the development and implementation of its National Cybersecurity Strategy and mentioned that a new cybersecurity law is pending approval. The Dominican Republic highlighted the integration of cybersecurity into its Artificial Intelligence Strategy, emphasizing eight principles, including respect for human rights. The Dominican Republic seeks to establish itself as a cybersecurity training hub and has appointed a Cyber Ambassador, the first in the Latin America and Caribbean region.
* *Ecuador* reported on the establishment of a cybersecurity committee focusing on the digital environment. With technical assistance from CICTE, Ecuador developed its National Cybersecurity Strategy. Ecuador has been collaborating with Cyber4Dev and CyberNet and is a subregional hub for the Andean region, as designated by Estonia. Ecuador noted that the United States has supported its participation in international forums and enhance its cybersecurity resiliency at the national level. Ecuador also highlighted participation in various CICTE programs, including the Cyber Women Challenge and She Secures.
* *Uruguay* highlighted the establishment of a national CERT as part of its new Digital Agenda. In addition to monitoring the cyber activities of more than ten national agencies, Uruguay has been focusing efforts to build capacity through academic programs and to train cybersecurity technicians, leading to the creation of a national cybersecurity curriculum for both public and private schools.
* *Bolivia* is actively working on a cybersecurity legal framework, including the development of a law for the protection of personal data. Additionally, Bolivia has established a system for recording incidents across all public entities and has provided guidelines for these entities to follow in addressing cybersecurity concerns.
* *The Bahamas* is currently drafting cybersecurity legislation that seeks to establish, among other things, a new cybersecurity agency. It is also working to publish a National Cybersecurity Strategy, the implementation of which will be led the Cyber Incident Response Team (CIRT). Moreover, the Bahamas is in the process of reviewing its data protection legislation and has undertaken numerous capacity-building efforts with diverse stakeholders. The country recently conducted its first cyber drill and hosted the CICTE’s Annual Cybersecurity Symposium to help build greater cybersecurity stakeholder awareness and capacity.

**Fourth plenary session**

A panel discussion was held on “Advancing the Implementation of CBMs in the Western Hemisphere.

* *Pablo A. Castro, Cybersecurity Coordinator, International and Human Security Division, Ministry of Foreign Affairs, Chile* noted the critical role of the CICTE Secretariat in supporting Member States, particularly in implementing cyber confidence-building measures through capacity building. He highlighted the need for states and other stakeholders to continue to exchange best practices. Castro suggested formalizing this engagement, potentially through structured meetings with other Member States, and proposed the development of an implementation plan for the eleven CBMs to guide collective action. Recognizing that Member States are at varying levels of cybersecurity maturity, Mr. Castro stressed the importance of regional cooperation. He further highlighted Chile’s new National Cybersecurity Strategy, which includes a strategy for international cooperation and private sector engagement. Mr. Castro also underscored the significance of sharing regional experiences at international fora such as the UN OEWG.
* *Daniela Ruiz Dominguez, Director for Cybersecurity and Conventional Weapons, Ministry of Foreign Affairs, Mexico* noted the growing tensions in other regions regarding the malicious use of information and communication technologies by state actors and related tension in cyberspace. She further noted that these trends could affect the OAS region and encouraged the Working Group to address them. She underscored that the Working Group serves as a platform for exchanging information, providing resources for best practices, conducting joint exercises, and facilitating joint training sessions. Ms. Dominguez welcomed the implementation survey proposed by the Chair, noting the importance of sharing the challenges faced by each country and working effectively with the private sector more generally.
* *Muriana McPherson, Director, National Data Management Authority, Guyana* emphasized that verifying and implementing CBMs can be labor-intensive, particularly for less developed countries, and proposed increased information-sharing in the portal among Points of Contacts. Ms. McPherson noted that Guyana has a draft National Cybersecurity Strategy (NCS) and cybercrime legislation largely in line with the Budapest Convention, as well as mutual legal assistance legislation. Additionally, a Data Protection Act was adopted in 2023. Guyana also has a Cyber Incident Response Team and a national cybersecurity schema to share information among public institutions in the event of a cyber incident. Plans are in place to amend legislation for reporting cyber incidents, with 24/7 monitoring of the government network in place. Ms. McPherson noted that over 75% of Ministries in Guyana have received awareness training, with over 50 individuals trained to train others. Ms. McPherson stressed the importance of having a champion at the senior level to support these efforts, citing the Prime Minister’s support for their first cyber risk assessment conducted last year.
* *Claudio Peguero, Ambassador, Advisor on Cyber-matters, Ministry of Foreign Affairs, Dominican Republic* highlighted his country’s adoption of a National Cybersecurity Strategy and designation of a Cyber Ambassador. He also highlighted that the Dominican Republic is building cyber diplomacy capacity, prioritizing the integration of a gender perspective, as well as capacity to strengthen critical infrastructure. Ambassador Peguero highlighted the participation of various stakeholders, including the private sector, in the development of projects related to cybersecurity legislation, communications, and infrastructure. He also stated that the Dominican Republic has issued a presidential decree providing for the reporting of incidents and responsible disclosure of vulnerabilities.

The delegations of Argentina, Chile, Colombia, United States and Uruguay then took the floor to provide reflections on the presentations made, and to comment on the work of the CBMS WG, particularly its role in the UN-OEWG discussions.

**Fifth plenary session**

A second panel discussion took place on “Encouraging and Promoting the Inclusion, Leadership, and Effective and Meaningful Participation of Women in Decision-Making Processes Linked to Information and Communications Technologies”.

* *Julia Rodríguez Acosta, Minister Consular, Permanent Mission of El Salvador to the United Nations, El Salvador* noted the recognition of differentiated experiences online between women and men and the importance of creating safer online environments. Given the role of women in international peace and security, Ms. Rodríguez emphasized the importance of building women’s capacity in cybersecurity, including supporting STEM programs and promoting gender inclusivity overall.
* *Belén Gallardo, Program Policy Advisor, International Cyber Policy Division, Global Affairs Canada* highlighted Canada’s commitment to advancing gender equality through domestic and foreign policy initiatives, including within the context of international development assistance. At the domestic level, efforts are being made to incorporate gender perspectives into cybersecurity-related issues, such as the National Cyber Security (NCS) framework and the Women, Peace, and Security agenda. Ms. Gallardo mentioned Canada’s support for the Women in Cyber (WiC) Fellowship, a program that facilitates the participation of more than 200 female diplomats and experts from diverse regions in events such as the Open-Ended Working Group (OEWG). Additionally, she highlighted Canada’s collaboration with CICTE to address online gender-based violence, and with the Inter-American Commission of Women (CIM) to develop model legislation and to raise greater regional awareness of gender sensitivity in cybersecurity.
* *Lisa Sharland, Senior Fellow and Director, Protecting Civilians and Human Security Program, The Stimson Center* identified the barriers that typically prevent women from participating in cyber discussions, such as the lack of skills, care responsibilities, and other systemic factors. Ms. Sharland indicated that addressing gender issues is a shared responsibility (not solely the responsibility of women), and that cybersecurity policies must effectively address gender disinformation and the gender impact of cyber incidents. Additionally, she emphasized the importance of considering human rights protections, especially regarding how data sets are quantified. Furthermore, addressing gender misinformation, online radicalization, and ensuring accountability for online behaviors are crucial components in promoting gender-inclusive cybersecurity.

The delegations of Argentina, Chile, Colombia, Ecuador and the United States then took the floor to encourage and promote the inclusion, leadership, and effective and meaningful participation of women in decision-making processes linked to information and communications technologies. In particular, beneficiaries of the Women in Cybersecurity (WiC) fellowship program acknowledged how the program played an important role in increasing their country’s participation in UN Processes.

**Fifth plenary session**

The morning of February 27, 2024 opened with the panel discussion “Exploring the Development of National Positions on the Applicability of International Law to Cyberspace.”

* *Gary Corn, Program Director & Adjunct Professor, Technology, Law, & Security, American University Washington College of Law* reflected on the issues related to the applicability of international law to cyberspace. Among other points, he highlighted that both states and non-state actors are often involved in cyberspace, with some engaging in situations deemed to be “armed conflicts.” As a result, appropriate rules need to be developed to address these different scenarios and actors in the cyberspace domain and that other existing rules under international law may be useful in this regard. He also touched upon the complexities of the cyber effects area, which involves the use of cyber tools to influence information spaces, including disinformation and propaganda.
* *Kimberley Raleigh, Senior Policy Advisor, Bureau of Cyberspace and Digital Policy, U.S. Department of State, United States* indicated that states should draft national positions regarding the applicability of international law in cyberspace. Without such positions, it is challenging for other states to understand where red lines are drawn and to avoid crossing them. The Compendium of voluntary national contributions on the subject of international law and cyberspace[[2]](#footnote-3) is designed to promote transparency and build confidence among states. Developing a national position involves consolidating views across different government agencies, including defense, foreign affairs, justice, intelligence, and homeland security. Ms. Raleigh emphasized the importance of involving experts in both cyber operations and international law during the drafting process.
* *Marcela Zamora Ovares, Head of the Department of Disarmament, Terrorism, and Organized Crime, General Directorate of Foreign Policy, Costa Rica.* In response to the 2021 cyberattack on public services, Costa Rica reinforced its cybersecurity and incident response capabilities, particularly regarding citizen and state data. Ms. Zamora stressed the importance of integrating international law, including human rights law, into cybersecurity frameworks efforts. Developing a national position on international law in cyberspace can also promote economic growth. Ms. Zamora shared Costa Rica’s experience of consulting various resources, such as the Tallinn Manual, in developing its national position.
* *Dr Andraz Kastelic, Security & Technology Programme, United Nations Institute for Disarmament Research (UNIDIR)* presented the challenges that can exist in developing national positions on international law in cyberspace, including a lack of awareness and capacity. UNIDIR is mandated with assisting UN States in developing and articulating national positions on how international law applies to state conduct in cyberspace and therefore offers capacity-building activities, such as scenario-based workshops for legal advisors. Additionally, UNIDIR conducts research and provides guidance on this topic.

The delegations of Argentina, Brazil, Canada, Chile, Colombia, Costa Rica, Dominica, Grenada, Ecuador, El Salvador, St Lucia, and the United States reflected on the development of national positions on the applicability of international law to cyberspace, and referenced the sovereignty issues that can be involved in such a process, including the inability to attribute when attacks are done through proxy.

**Seventh plenary session**

The presentation on the Cyber Incident Severity Schema by Patrick Kyhos, Director for Operations and Incident Response at the White House Office of the National Cyber Director, was removed from the agenda due to a scheduling conflict.

**Eighth plenary session**

Member States discussed how to leverage the existing CBMS Points of Contact (POC) directory with the UN Global POC Directory:

* The *United States* mentioned that discussions within the Open-ended Working Group have recognized the importance of coherence between regional directories and the global directory and suggested that it may be appropriate for the Working Group to discuss this issue now while the UN POC directory is still under development (rather than after its creation). The United States also emphasized the importance of maintaining consistent information across both platforms and suggested the adoption of a practice wherein OAS Member States that wish to nominate the same person(s) for the UN POC directory who are current OAS POCs could expressly authorize CICTE to transmit those contact details to the UN. The United States also proposed that CICTE conduct regular updates to the CBMS PoC network to ensure that the information remains current, possibly through periodic invitations to update PoC information.
* *Chile* commented on the operationalization of the PoCs of the CBMs Working Group and supported the CICTE Secretariat’s proposal of hosting webinars among the POCs to facilitate communication and engagement across Member States. Chile also indicated the need for further discussion around the establishment of the UN global directory. Additionally, Chile suggested that Member States could choose whether CICTE should send PoC information to the UN or if countries should do so themselves.
* *Mexico* suggested the possibility of having countries assign the same PoCs to the CBMs Working Group as to the UN global directory. Mexico emphasized the benefits of having officials familiar with the dynamics of this regional PoC directory, which would help them leverage best practices, streamline processes, and avoid task duplication. Mexico also expressed openness to letting countries decide whether or not to share their PoC information for the global directory through CICTE.
* *Brazil* encouraged greater synergy between the two networks and encouraged the CICTE Secretariat to stay attentive to UN developments in the matter.
* *Colombia* also noted the importance of greater synergy to facilitate coordination and suggested continued discussion of the matter through the Working Group.

**Election of authorities**

The meeting then proceeded to the election of officers for the Sixth Working Group on Cooperation and Confidence-Building Measures in Cyberspace.

The delegation of Chile nominated the Government of Dominican Republic to chair the Sixth Working Group Meeting and the motion was approved by acclamation. Ambassador Claudio Peguero, Advisor on Cyber-Matters, Ministry of Foreign Affairs of the Dominican Republic, accepted the nomination on behalf of his country and expressed his government’s appreciation for the confidence bestowed.

The delegation of Colombia then nominated the Government of Canada for the position of Vice Chair. The nomination was also approved by acclamation. Ms. Belén Gallardo, Program Policy Advisor, International Cyber Policy Division, Global Affairs Canada, accepted the nomination on behalf of her government.

**Closing Session**

The Chair thanked all delegates for their participation and summarized the key proposals made during the meeting:

1. Development of training curricula for diplomatic academies in OAS Member States;
2. Development of a regional workplan to support implementation of agreed-upon OAS Cyber CBMs;
3. Holding of informal meetings of the OAS CBMs WG at the UN prior to the sessions of the OEWG;
4. Organization of roundtables to help Member States develop national positions on the applicability of international law to cyberspace;
5. Promoting synergies between the OAS CBMs POC Directory and the UN Global POC Directory.

There being no other business to discuss, the meeting was adjourned at 12:45 p.m.

CICTE01702E01

1. The delegation of Brazil noted the absence of interpretation in all four (4) official language of the OAS, which negatively impacts full participation by all Member States. The CICTE Secretariat responded that meetings of the Working Group have historically been held only in English and Spanish due to budgetary constraints. [↑](#footnote-ref-2)
2. Official compendium of voluntary national contributions on the subject of how international law applies to the use of information and communications technologies by States submitted by participating governmental experts in the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security established pursuant to General Assembly resolution 73/26 \_ [A-76-136-EN.pdf (un-arm.org)](https://front.un-arm.org/wp-content/uploads/2021/08/A-76-136-EN.pdf) [↑](#footnote-ref-3)