GFCE Regional Meeting in the Americas & Caribbean 2023 - Report

GLOBAL FORUM ON CYBER EXPERTISE

Organization of American States

GFCE Regional Meeting in the Americas 2023

San Jose, Costa Rica, 5 June 2023

The meeting was organized by the GFCE Regional Hub for the Americas and the Caribbean as a satellite event to RightsCon. The Hub provides practical guidance, expertise, and support to cyber communities, including regional organizations, private sector entities, institutions, and governments. It also facilitates access to the GFCE's global network for countries seeking support.

The objective of this year's Regional Meeting in the Americas was to discuss the role of the GFCE in Latin America and the Caribbean and how to best coordinate capacity building efforts in the region. It provided an opportunity for participants from the region to connect and engage in conversations about existing gaps in cyber capacity building, share good practices, and prioritize their needs for the future. Specific attention was given to gender aspects and cyber workforce development in the region.

Central to this year's regional meeting were GFCE's efforts in improving coordination. Notably: i) reinforcing a demand-driven approach through expansion with regional (locally based) liaisons and offices and ii) mobilizing resources for cyber capacity building through the organization of the Global Conference on Cyber Capacity Building (GC3B) in 2023. It is in the context of regional cooperation, that the Secretariat of the GFCE, together with the Secretariat of the Inter-American Committee Against Terrorism (CICTE) of the Organization of American States (OAS) -which is the GFCE Regional hub for the Americas and the Caribbean region - organize the GFCE Regional Meeting in the Americas 2023.

The meeting commenced with key remarks from Alison August Treppel, Secretary of OAS/CICTE, Chris Painter, President of the GFCE Foundation, and Nicholas Natale, Senior Program Manager of Global Affairs Canada. They emphasized the significance of cybersecurity capacity building (CCB) in the region and the need for increased collaboration within countries and communities. They also highlighted the importance of countries voicing their needs, contributing to their own benefit, and effectively implementing the contributions of various donors to enhance CCB in the region. Additionally, the involvement of individuals in cybersecurity was emphasized, highlighting that it is not just a security issue but also important to enhance the understanding of digitization and its associated challenges.

During the presentation of the regional hub for the Americas and the Caribbean, representatives from the GFCE Secretariat and the Regional Hub (Valentina Name, Velimir Radicevic, Manuel Precioso Ruiz and Tereza Horejsova) provided updates on the activities that took place throughout the past year. They also shared information on how to engage with the GFCE, the functions of the clearing house mechanism, and the GFCE's role in coordinating cybersecurity capacity building through/thanks to the unique position of the GFCE in connecting the dots between regional hubs, and GFCE's members, and partners was also emphasized.

Subsequently, the session continued to cover one of the GFCE's main working mechanisms, the Working Groups. This was achieved thanks to interventions of representatives of three of these: Working Group A focused on "Cyber Security Strategy & Policy," Working Group B on "Cyber Incident Management and Critical Infrastructure Protection," and Working Group C on "Cybercrime." The discussions centered around the work accomplished within the respective working groups and their way forward. Firstly, WG A highlighted the importance of cyber-diplomacy norms, cybersecurity strategies, and the support provided

by the WG in developing useful tools that helps key processes such as the implementation of national strategies. WG B discussed the work that is being carried out for developing a practical guide for tabletop exercises, the value of discussing best practices and challenges when it comes to cybersecurity incident management and incident reporting maturity frameworks and presented upcoming in-person and online engagements of the WG. Finally, WG C presented the benefits of getting involved in the GFCE Working Groups, emphasizing useful and valuable initiatives that the WG has worked over the past year, such as a mapping initiatives for collaboration and shared an example of how the WG helped to support the Gambia's cybercrime needs through the GFCE's Clearing House Function

Moreover, the meeting delved deeper into regional priorities for cybersecurity capacity building. In particular, the focus was placed on workforce development with presentations by a representative from Chile (Pablo Castro), and a representative from the OAS/GFCE Regional hub (Valentina Name). One of the highlights from this session was when Chile shared their valuable experience in developing the Chilean cybersecurity strategy, emphasizing its early adoption in 2017 with a strong focus on cybersecurity culture and education. Cybersecurity became a strategic component integrated across various ministries, with active involvement from the private sector. Regardless of remaining challenges, such as the absence of dedicated legislation and a national agency, Chile expressed optimism about the ongoing development of an updated strategy that includes international cooperation aspects and extends until 2028.

The discussion further explored regional priorities in cybersecurity, highlighting the importance of cyber intelligence and the growing significance of artificial intelligence (AI). Participants agreed on the need to prioritize cybersecurity in educational curricula and increase basic awareness, exposing the misconception that it is solely an IT problem. Bridging gaps and fostering collaboration among decision-makers, as shown by Panama's experience, were considered crucial. The GFCE and the Americas and Caribbean hub were identified as potential facilitators to bridge these gaps. Additionally, engaging university students and involving private sector actors from the higher education sector were emphasized as essential steps toward strengthening cybersecurity in the region.

The final panel focused on the challenges and practical steps to promote gender mainstreaming in cybersecurity capacity building. The GFCE and the GFCE Regional hub presented global and regional strategies, initiatives, and good practices aimed at integrating gender and diversity perspectives into CCB as well as an overview of gender concepts and their impact on the cybersecurity field.Also, the gendered nature of cybersecurity was emphasized, as well as the existing workforce gap, supported by survey results from 2021 and 2022, and the different threats with a gender perspective, particularly around gender-based violence. In this regard, one of the main recommendations was to simplify communication to communities and countries to enhance understanding of cybersecurity and its gender-related impact.

In conclusion, the need for guidance on how the private sector, public sector, and institutions can promote and communicate gender inclusion in CCB was identified. A call to action was made to bring together LAC members and partners to pool resources for the benefit of countries in need. Additionally, it emphasized the importance of including in the Regional Agenda for the GC3B global meeting the need for cross-regional learning to support the region's work and foster global synergies.