Report

GFCE Regional Meeting for the Americas and the Caribbean 2024

September 9, 2024
Washington D.C., United States

Organization of American States (OAS)
Headquarters, Washington D.C., USA

OAS | CICTE | GFCE Global Forum on Cyber Expertise | REGIONAL HUB FOR THE AMERICAS

Supported by:

GFCE Regional Meeting for the Americas and the Caribbean 2024

Report

No. of attendees: 115

In an era marked by increasing cybersecurity threats and technological advancements, the **4th GFCE Regional Meeting for the Americas and the Caribbean** convened in Washington, DC, to address these critical issues. Since the Organization of American States (OAS) became a member of the Global Forum on Cyber Expertise (GFCE) in 2015 and established the Latin America and Caribbean (LAC) Hub in 2018, the objective has been to empower and strengthen cyber communities across the region. This meeting provided a collaborative platform for stakeholders from governments, private entities, and academia to discuss strategies for enhancing regional cybersecurity resilience. Participants engaged in discussions focused on the rise of ransomware, the impact of emerging technologies, and the importance of fostering inclusive cybersecurity practices. The meeting underscored the necessity of cohesive efforts to build capacity, promote public-private partnerships, and address the unique challenges faced by the region.

The meeting featured a series of panels and presentations emphasized the need to continue building capacity in the region, with a special focus on emerging technologies and their discourse across the Americas. The following topics were discussed in depth:

- **Identification of Capacity and Needs for AI Governance in the Americas and the Caribbean:** This session explored how governments and the private sector in the region are harnessing the potential of AI while mitigating risks and improving cybersecurity.

- **Integrating National AI Strategies into National Cybersecurity Strategies:** The discussion centered on the importance of digital protection across the region and how new technologies can be best adapted within existing cybersecurity frameworks.

GFCE Regional Meeting for the Americas and the Caribbean 2024

Report

Report

- **Research presentation of the ICT4Peace Foundation Report, "Advancing Global Digital Governance:** Opportunities, Challenges, and Future Directions in ICT State Behavior and Multilateral Frameworks." This session featured a pre-launch presentation of the ICT4Peace Foundation's report, which outlines critical insights into global digital governance and its implications for state behavior.

- **Showcase of Working Group E "Emerging Technologies" and Its Contributions to the Region:** This session highlighted ongoing projects involving emerging technologies from Canada, Ghana, Amazon Web Services (AWS) (representing the private sector), and the OAS Executive Secretariat for Integral Development (SEDI), offering a regional organization's perspective.

- **Addressing Challenges, Sharing Best Practices, and Crafting Solutions for Gender Diversity in Cybersecurity:** Panelists discussed actionable strategies and solutions for enhancing gender diversity within the cybersecurity workforce in the Americas, examining how diversity can strengthen the sector's ability to address cybersecurity threats and mitigate risks associated with emerging technologies.

GFCE Regional Meeting for the Americas and the Caribbean 2024

Report

Cybersecurity Challenges in Latin America and the Caribbean

Ransomware and cyber-attacks were identified as significant threats to the region, with stakeholders emphasizing the need for unified responses and stronger frameworks. Panelists highlighted the importance of sharing expertise, developing policies, and aligning regional efforts to combat these growing cyber threats. Discussions revolved around establishing guidelines for incident response applicable to both the public and private sectors and fostering public-private partnerships to enhance cybersecurity resilience.

Emerging Technologies and Artificial Intelligence (AI)

The rapid adoption of AI across the region has opened new opportunities for innovation but also poses significant risks in the cybersecurity landscape. Experts discussed the need for ethical AI frameworks and international collaboration to address AI-related challenges. Key areas of focus included the development of infrastructure and technology, ethical principles in AI development, and private sector engagement to ensure that AI is both beneficial and secure. A critical takeaway was the importance of viewing AI as a public technology that requires interoperable solutions across sectors and borders.

Work Plan for 2024

The meeting presented an overview of the 2024 Work Plan, focusing on enhancing cyber capacity building across the Americas and the Caribbean. The work plan outlined efforts to:

Reduce duplication of efforts through tools like the Cybil Portal, which promotes collaboration as well as knowledge sharing among the GFCE different stakeholders.

Engage donors and implementors more effectively to align resources with regional needs.

Enhance regional collaboration through the Latin American and Caribbean (LAC) Hub, which plays a crucial role in connecting actors, facilitating knowledge exchange, and ensuring equitable access to resources.

Ecuador's recent membership in the GFCE was also recognized, with the meeting underscoring the importance of promoting regional efforts through various GFCE tools and channels.

GFCE Regional Meeting for the Americas and the Caribbean 2024

Report

Report

Public-Private Partnerships and Sectoral Dialogue

There was a strong emphasis on fostering deeper dialogue between the government and private sectors, particularly in creating industry standards that are adaptable and applicable to regional contexts. International organizations were called upon to facilitate these discussions, ensuring that cybersecurity policies are neutral and inclusive of both civilian and military uses of technology. These conversations are seen as vital to bridging the gap between research and the practical application of AI and cybersecurity technologies.

Research presentation of the ICT4Peace Foundation Report, "Advancing Global Digital Governance: Opportunities, Challenges, and Future Directions in ICT State Behavior and Multilateral Frameworks."

The session presented the overview of the ongoing research that is underway by the OAS and ICT4Peace titled "Advancing Global Digital Governance." This research analyzes the current international ICT governance landscape, emphasizing key multilateral processes within the United Nations system, including the Open-Ended Working Group on the security of and in the use of ICTs (OEWG), the World Summit on the Information Society (WSIS) process, and the emerging Global Digital Compact (GDC). The report aims to serve as a valuable resource for governments and stakeholders, highlighting challenges and opportunities in digital governance while emphasizing the need for multistakeholder participation and international cooperation on ICT-related issues.

Showcase of Emerging Technologies (WG E)

Speakers from various regions and sectors, including the private sector (Amazon Web Services), the Organization of American States, Canada, and Ghana, discussed the importance of aligning emerging technologies with cyber capacity-building efforts. The use of AI, blockchain, and quantum computing was highlighted as crucial for improving incident response, stakeholder management, and cybersecurity frameworks. Training and accreditation initiatives were also spotlighted, especially in Ghana, where a database of cybersecurity professionals is being developed to ensure a skilled workforce.

GFCE Regional Meeting for the Americas and the Caribbean 2024

Report

Report

Gender Perspectives in Cybersecurity

The meeting also focused on gender equality in the cybersecurity workforce. Key outcomes from the Global Survey by OAS/CICTE Cybersecurity Section highlighted improvements in gender representation over the past five years, although challenges such as sexual harassment and wage disparities persist. Panelists emphasized the need for inclusive cybersecurity policies and programs, such as Canada's Women in Cyber Fellowship Program, which aims to address historical gender disparities. Chile's initiatives in public-private partnerships and gender parity in executive roles were also discussed as models for regional adoption.

GFCE Regional Meeting for the Americas and the Caribbean 2024

Report

Conclusion

The 4th GFCE Regional Meeting for the Americas and the Caribbean underscored the region's commitment to enhancing cybersecurity capacity and collaboration. Discussions reflected the pressing need for robust incident response frameworks, the development of public-private partnerships, and the integration of ethical standards in emerging technologies like AI. The research presentation of the ICT4Peace Foundation's report highlighted the importance of multistakeholder participation and international cooperation in addressing the challenges of digital governance. Additionally, the significance of gender inclusion in cybersecurity, along with the role of international cooperation and donor support, were recurring themes throughout the meeting. Moving forward, the region must continue to align its strategies to address both current and future challenges while ensuring that capacity-building efforts are impactful and inclusive. The event concluded with a call for ongoing dialogue and cooperation to achieve these goals, reinforcing the significance of the GFCE as a trusted partner for coordinating cybersecurity advancement in the region.

OAS | CICTE | GFCE Global Forum on Cyber Expertise | REGIONAL HUB FOR THE AMERICAS

Supported by:

Report

GFCE Regional Meeting for the Americas and the Caribbean 2024

September 9, 2024
Washington D.C., United States

Organization of American States (OAS)
Headquarters, Washington D.C., USA

OAS | CICTE | GFCE Global Forum on Cyber Expertise | REGIONAL HUB FOR THE AMERICAS

Supported by: