Open-Ended Working Group on security of and in the use of information and communications
technologies 2021-2025 (OEWG)
Third Substantive Session- July 2022

Presentation of the Organization of American States on experiences in the area of capacity-building in the field of information and communications technology (ICT) security

Distinguished, Chair of Open-Ended Working Group on security of and in the use of Information and Communications Technologies of the United Nations, Ambassador Burhan Gafoor,

Distinguished delegates,

I would like to begin by thanking the Chair for the invitation to speak today on behalf of the Organization of American States (OAS) and its Inter-American Committee against Terrorism (CICTE).

The OAS and the UN have had a fruitful partnership on key cybersecurity issues. In particular, in 2019, the OAS was honored to participate in UNIDIR’s 2nd International Security Cyber Workshop Series that focused on the role of regional organizations in strengthening cybersecurity and stability. The consensus then was that regional cybersecurity efforts should involve awareness raising, capacity building, confidence building and cooperation, and that regional organizations should develop responses that meet their region’s unique social, economic and security priorities and challenges. These findings we still find to be valid today.

Chair, regional organizations such as the OAS have long acted as interlocutors for implementing UN mandates at the regional level and for helping to ensure that Member States are fulfilling their various international obligations. This is particularly true for cybersecurity capacity building where the OAS has been working for nearly 20 years with different UN agencies and bodies, including this one, to help ensure that international responses take into account the cybersecurity challenges --and related social, economic and security considerations-- faced by our Hemisphere

Chair, OAS Member States have recognized the vital role of building a culture of cybersecurity for the prosperity of the region since 2004.

As such, we would like to highlight just some of the key initiatives we have developed over the past two decades and then offer a few lessons that might be helpful for Member State deliberations over the coming days.

First, since 2017, and with the financial support of Canada, the United States and the Government of the Netherlands, and the United Kingdom, OAS/CICTE has offered cyber diplomacy courses to
strengthen member states knowledge of the UN and other cybersecurity processes, particularly within the United Nations' First Committee.

These courses, which have been delivered to nearly 90% of our Member States over the past 5 years, have also provided an overview of the normative framework of responsible state behavior promulgated by the UN and relevant legal frameworks, as well as tools to assist in cross-border digital crime cooperation, including the UNODC’s *Practical Guide for Requesting Electronic Evidence Across Borders*. We believe that this kind of information will equip our member states to more proactively engage in dialogues such as this. In fact, I am very proud, Chair, to note that many delegates here today from the region are alumni of our cyber diplomacy training.

Another key initiative is that in 2017, the OAS approved Resolution CICTE / RES.1 / 17 which established a Working Group on Measures to Promote Cooperation and Trust in Cyberspace. As a result of the establishment of this working group, six regional measures to promote cooperation and confidence in cyberspace have been approved, two of which include:

- Designation of a national point of contact at the policy level that can discuss the implications of hemispheric cyber threats.
- Provision of information on cybersecurity policies, such as national strategies, white papers, legal frameworks, and other relevant documents;

As part of the implementation of the agreed CBMs, the Technical Secretariat developed a web portal to manage the cyber policy points of contacts of the OAS Member States and provide them 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.

OAS/CICTE also has in place an initiative called the CSIRTAmericas network, which is comprised of 33 national Cybersecurity Incident Response teams and 148 experts from 21 countries of Latin America and the Caribbean. Member States belonging to the network receive 24/7 threat intelligence aggregated from third party sources at no cost. Through this platform we also organize training for policymakers and incident handlers, which allows them to stay updated on new developments and threat identification tools, among other issues of interest.

Additionally, we have taken note of member states interest on the promotion of gender and have included in our full written statement a description of two of our youth and gender initiatives and on the screen an overview of our current gender initiatives being delivered with the support of the Government of Canada.

The development of two youth and diversity-focused initiatives: The “Creating a Cybersecurity Pathway” training and the “Cyber Women Challenge”. The first, has impacted over 500 young people from the Americas and the Caribbean, introducing them cybersecurity fundamentals and showcase different cybersecurity career opportunities for their professional development. The latter has enabled 1500+ women from our region to gain specific skills for a growing workforce that requires more diversity and benefits from women’s participation to respond to cybersecurity incidents and create inclusive solutions to a growing threat landscape.
As I said earlier, we have learned many lessons from nearly two decades of implementing these and other cyber-capacity building initiatives, but one lesson, Chair, has always been abundantly clear. And that is that cybersecurity is a shared responsibility between government, the private sector, and civil society that is built on trust, mutual respect, and understanding.

At the OAS, we have built lasting connections with private entities such as Cisco, Citi, Trend Micro, Microsoft, and AWS, as well as with civil society organizations such as Anti-Phishing Working Group, Forum of Incident Response and Security Teams (FIRST), Global Partners Digital. We work together to ensure that the impact of our joint efforts respects and recognizes each country’s reality and fundamental human rights, while enabling burgeoning cybersecurity capabilities to emerge and strengthen.

This type of cooperation among organizations and countries, Chair, can be duplicated outside of our region and structured to flow north-south, north-north, and south-south, giving beneficiaries the opportunity to learn not only from more advanced countries, but also from their regional counterparts who may have faced similar challenges with very similar environments. For this reason, OAS/CICTE was pleased to be nominated as the Regional Hub for the Global Forum on Cyber Expertise, given the GFCE’s role as a global platform comprising of governments, international organizations, non-governmental organizations, civil society, private companies, the technical community, and academia.

Another key lesson is that although the COVID-19 pandemic had restricted considerably in-person activities, online trainings did prove to be allow us to reach larger audiences benefiting from the cyber capacity building activities organized. In our case in particular, webinars have been organized around issues relevant and timely issues, drawing from our close list of experts and partners to discuss them in a way that policymakers and the general population can understand.

Finally, it is important to remember that capacity building should take into account current threats as they evolve and be able to pivot accordingly. For example, this year one of our cybersecurity reports identified that ransomware was one of the main reasons for concern for institutions in Latin America and the Caribbean, accelerated by the pace of modern cybercrime campaigns and gaps in security mechanisms due to the need to access more data remotely.

As such, the OAS/CICTE is developing a series of capacity building efforts to support member states ability to address ransomware, for example a white paper with AWS and a series of webinars for the general public. Chair, today the threat might be ransomware, tomorrow it may be something else, what we hope to emphasize is the need for continued information sharing, a task that is greatly facilitated by multi-stakeholder involvement.

We would like to close by stating that regional bodies such as the OAS will continue to work jointly on training, especially with regards to cybersecurity exercises, best practices for incident handling and management of cybersecurity aspects across different stakeholders, such as policy.
representatives, security forces. We believe that the exchange of experiences including the implementation of CBMs across regions and the facilitation of cross-regional dialogue will only be to the benefits of the UN member states.

Chair, capacity building is not a new tool for conflict resolution, but more than ever, it is the path towards building greater consensus and international cooperation in cybersecurity. Considering the dynamic and borderless nature of cybersecurity, regional and international capacity building is vital to adequately respond to evolving cyber threats and vulnerabilities. We value and appreciate UN resolutions and other international instruments that continue to recognize the role of regional organizations and congratulate you again Chair for creating this important space and platform to share and coordinate. OAS/CICTE reiterates its continued commitment to collaborating with the United Nations to create a more secure cyberspace.

Thank you Chair.