Contribution to the Sixth Substantive Session of the Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information Technologies for Criminal Purposes 2021 - 2024 (AHC)

On behalf of the Global Forum on Cyber Expertise (GFCE) Foundation, we welcome the opportunity to submit our contribution to the Sixth Substantive Session of the Ad Hoc Committee (AHC) to Elaborate a Comprehensive International Convention on Countering the Use of Information Technologies (ICTs) for Criminal Purposes 2021-2024.

Referring to the draft text of the convention, as per A/AC.291/22, the GFCE wishes to make recommendations for Member States' consideration on Chapter VII Technical assistance and information exchange, Article 54. Technical assistance and capacity-building, on how to best leverage multistakeholder efforts and contributions in combatting cybercrime through providing technical assistance and capacity-building.

We will also reiterate how the GFCE can serve as a preferred platform to support the development and implementation of capacity building provisions agreed by States in the framework of the new Convention, through the Forum's unique position and key role in facilitating and coordinating capacity building efforts, made possible by its neutrality, community-driven, and action-oriented approach.

GFCE mission

The GFCE is a neutral multistakeholder community of over 190 members and partners including UN member states, UN entities, as well as international and regional organizations such as INTERPOL, the Council of Europe, and the World Bank. The GFCE also counts industry bodies and private sector actors, civil society, technical organizations and academia amongst its Partners, in a platform dedicated to the global coordination and promotion of cyber capacity building.

The mission of the GFCE is to strengthen international collaboration on cyber capacity building and expertise globally – this involves developing and exchanging understanding on best practices, promoting what has worked – and encouraging the development and adoption of capacity building at the domestic, regional and international levels. Since 2015, the GFCE has been harnessing and consolidating existing capacity building efforts through its ecosystem to strengthen coordination, facilitate knowledge sharing, and connect assistance requests with support or resources.

GFCE Working Group on Cybercrime

The GFCE's multistakeholder community come together to share, shape and form knowledge on specific issues in thematic Working Groups. The Working Group (WG) on Cybercrime is one example of the ways in which the GFCE helps to bridge divides between stakeholder groups and contribute to promoting general awareness amongst policymakers, practitioners, institutions, and organizations of capacity building activities, tools and frameworks for addressing cybercrime.

The Working Groups also serve as an important venue for its members to exchange views on emerging threats and explore mitigation measures, functions as an incubator for the collaborative development of knowledge products & circulation of best practices and serves to build trust and promote partnerships amongst its members. For example, the "Cybercrime Series" provides a platform for members to discuss trends and developments in cybercrime and aims to develop a common understanding on respective developments and identify successful policies, practices and ideas for capacity building. The series has covered topics such as ransomware, the use of cryptocurrencies and virtual assets for criminal use, and combatting Online Child Sexual Exploitation and Abuse. The most recent regional session on "Capacity Building in the context of AHC negotiations: Reflections from the LAC region", provided a platform for discussions and sharing experiences on capacity building in relation to AHC negotiations, through a regional lens. Regional organizations, civil society and states

reflected on how the existing inter-American cooperation mechanisms provided an a-priori baseline for regional cooperation, and how LAC interests and values were represented in the current text of the Convention.

Multistakeholder role in technical assistance and capacity building

Reiterating that combatting cybercrime is a multidisciplinary enterprise that requires the cooperation of various stakeholders operating across different policy and operational domains, cooperation between states and civil society, the private sector and academia is vital when addressing the transnational challenges of malicious use of ICTs and for protecting users of these technologies.

The GFCE therefore supports proposals made by several of its Members to streamline the language in Article 54, paragraph 8 and explicitly acknowledge the role of international and regional organizations in providing technical assistance and capacity building, which extends beyond operational and training activities. Paragraph 8 could also be further streamlined with other proposed paragraphs of the chapter and refer to "other relevant organizations and stakeholders" alongside international and regional organisations to avoid the risk of pre-emptively excluding relevant actors. Recognising the added value and differentiated roles stakeholders are called to play in the design, delivery and implementation of technical assistance and capacity building will allow recipients to benefit from more specialized, tailored support. It will allow for more flexibility both for recipients, as well as for donors.

Capacity building is a fluid concept requiring a flexible approach that fully takes into account the needs of different actors involved in combatting cybercrime, as well the challenges met across the design and delivery of such initiatives. In this respect, it would be advisable for the future Convention not to be too prescriptive on the delivery of capacity building. The Convention would benefit from acknowledging that different needs stemming from the different actors require various types of assistance, that would be best provided by distinct, specialized organizations. International organizations such as UNODC, INTERPOL, the World Bank and the GFCE are already playing an important role in the coordination and facilitation of technical assistance and capacity building. The future Convention could emphasise and leverage on existing efforts, whilst underlining the complementarity between the different mandates of international organizations providing technical assistance and capacity building. The GFCE is well placed to support this process through its coordination role, and benefiting from its multistakeholder community.

Conclusion

With Chapter VII on Technical Assistance being considered as one of the most significant of the future Convention, States signal that capacity building is key in narrowing the gaps in capacities between members. Ultimately, the implementation of the Convention in its fullest will depend on states capacities to implement it and thus to prevent, investigate, prosecute, adjudicate and engage in judicial international cooperation as it relates to cybercrime.

The GFCE maintains its view that defining specific roles for organizations risks discouraging collaborative approaches to capacity building, pre-emptively excluding actors from core processes and mechanisms, and ultimately may be challenging to implement especially given the multi-disciplinary and multistakeholder nature of the capacity building ecosystem.

The GFCE encourages that non-State actors continue to be provided avenues to share input and advice especially in the context of capacity building. As effective cyber capacity building requires open channels for dialogue and cooperation between both state and non-state actors, discussions on capacity building must be premised on an inclusive, multistakeholder process.

Given the GFCE's ecosystem and its established multistakeholder network, the UN and all Member States are encouraged to engage with the GFCE as a way of linking multilateral and state-centric processes with the expertise, knowledge and resources of the private sector, civil society, academia, and the technical community.