Contribution to the Fifth 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 submit the following contribution to the Fifth 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.

In this contribution, we would like to highlight the importance of principle-based technical assistance and capacity building and of multistakeholder participation in combatting cybercrime. We will further detail how the GFCE can serve as a platform to support the development and implementation of capacity building measures 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.

The GFCE is a neutral multistakeholder community of over 180 members and partners including UN member states, UN entities such as the International Telecommunications Union (ITU), United Nations Office on Drugs and Crime (UNODC), and the United Nations Institute for Disarmament Research (UNIDIR), as well as international and regional organizations, private sector, civil society and academia, 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.

Principle-based capacity building

Chapter V on Technical Assistance of the consolidated negotiating document (CND) is considered as one of the main chapters of the future Convention, alongside Chapter I defining the use of terms and determining the scope of application, and Chapter IV laying down the basis for international cooperation. The implementation of the Convention in its fullest will depend on states capacities and capabilities to implement it and thus to prevent, investigate, prosecute, adjudicate and engage in judicial international cooperation as it relates to cybercrime. Principle-based capacity-building is proposed not only as a means of putting in place checks and balances but also better align cyber capacity building with international development. [1]

Echoing several state parties and multistakeholder views expressed during the 5th substantive session of the AHC, the GFCE recommends that the future Convention builds upon the already strong foundation and existing work in the field. For example, the effective participation and involvement of all stakeholders and ownership, sustainability and transparency in capacity building are some of the core principles of the GFCE's Delhi Communiqué on the **Global Agenda for Cyber Capacity Building**, endorsed by the GFCE community. These principles were based on general principles for development and capacity building set out in the Busan Partnership for Effective Development Co-operation, directly linking thus cyber capacity building with international development principles.

The GFCE also reiterates that the prevention and response to cybercrime and measures to enhance cybersecurity are mutually reinforcing. Though separate and distinct subject matter, lessons and

[1] "How can the cybercrime convention adopt a strategic approach to cybercrime capacity building and protect against potential harms and misuses?" Chatham House

parallels can also be drawn from the UN First Committee, in particular the principles for capacity building as outlined in the 2021 report of the OEWG on ICTs in the context of international security. The report, endorsed by all UN Member states indicates that cyber capacity building should be guided by 11 principles organised in three categories: process and purpose; partnerships; and people. The principles in the new Cybercrime Convention could mirror those agreed in the OEWG, clearly underlining the participation and role of Multistakeholder actors.

Multistakeholder participation

Combatting cybercrime is a multidisciplinary enterprise that requires the cooperation of various stakeholders operating across different policy and operational domains. The 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 and empowering users of these technologies. This has been reflected thus far in the modalities for inclusion and participation of non-state actors during the negotiating process itself. The GFCE would therefore encourage to strengthen the acknowledgement of the multistakeholder approach throughout the new Convention, particularly underlining the added value and differentiated roles stakeholders are called to play in the design, delivery and implementation of technical assistance and capacity building.

GFCE's mechanisms and tools reflect its multistakeholder by design community and contribute to a better understanding of countries' needs and priorities, support a tailored, targeted approach for capacity building and to inclusive, coordinated, and effective capacity building efforts in general.

GFCE Working Groups

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 reducing the general lack of awareness amongst policymakers, practitioners, institutions, and organizations of capacity building activities, tools and frameworks for addressing cybercrime.
The Working Groups are also a 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. The "Cybercrime Series" developed by the WG on Cybercrime 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.

GFCE Research Agenda

Within the Working Groups, the community identifies knowledge gaps and prioritizes them, resulting in a bi-annual Global Capacity Building Research Agenda. Through the GFCE's Research Agenda, knowledge gaps related to offences covered by the future Convention or other research programs can also be proposed, engaging the academic community to support informed practical strategies and solutions by providing data and analysis.

Cybil Portal

The GFCE encourages States to provide transparent information on measures taken to address cybercrime through capacity building, including sharing challenges faced and best practices related to the establishment and implementation of capacity building efforts. Divergences in information on the levels of development and implementation of capacity building measures can have a negative effect on the ability and expectations of stakeholders engaged in cyber capacity building, particularly at the

regional level. To support this, the UN could encourage States to share information, through repositories such as GFCE's Cybil Portal – a global, open and free knowledge repository with information on already over 800 cyber capacity projects, and over 300 tools and resources. By providing accessible information and improving transparency on capacity building projects, Cybil contributes to stronger, more efficient global cyber security and cybercrime capacity-building.

GFCE's Match Making / Clearing House function

The GFCE's Match Making/ Clearing House (CH) mechanism refers to requesting countries identifying themselves where support is needed based on their specific situation, and the GFCE connecting those actors with GFCE members and partners that can provide targeted capacity building support. The GFCE provides thus a space for international implementing partners to connect with the requesting country to accurately identify their capacity needs and connect with others working in the country/region to avoid duplication of efforts and ensure efficient use of resources. Eg with Sierra Leone the GFCE is working to support the rollout of the national cybercrime awareness program. The CH provides a means to bridge the divide between provider/ recipient of capacity building, and allows different actors to hold different roles in specific contexts. Moreover, the mechanism foresees a built-in strong local stakeholder involvement in all the stages of developing and implementing the capacity building response which promotes ownership, sustainability and accountability.

Regional Approach

With the establishment of GFCE Regional Offices and designation of Regional Liaisons over the last two years, the GFCE supports regional actors in CCB in the process to accurately identify needs, define a regional agenda and bring this to the global Community. For example, through the AU-GFCE collaboration, combatting cybercrime and child online protection have been identified as priority areas by the Africa Cyber Experts (ACE) community, and converted into Knowledge Modules.

Conclusion

While negotiations within the context of the UN and AHC are multilateral and state-led processes, 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.

The GFCE advises for the prospective Convention not to be too prescriptive on the delivery of capacity building and not to designate a specific organization as the primary mechanism and coordinator for technical assistance and capacity building. While acknowledging that UNODC has an important role both in the delivery and coordination of technical assistance and capacity building, other organisations also have important roles and experience in such coordination and facilitation (e.g. INTERPOL, EUROPOL, the World Bank). Moreso, given the dispersed and transnational nature of cybercrime, there is still a need for these organizations to engage with stakeholders outside of traditional cybercrime communities. The GFCE maintains its view that defining overly specific roles risks discouraging collaborative approaches to capacity building, pre-emptively excluding actors from core processes and mechanisms, and ultimately may be challenging to implement.

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.