Contribution to the Third 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)

Contribution of the Global Forum on Cyber Expertise (GFCE)
Tuesday 30 August 2022

On behalf of the Global Forum on Cyber Expertise (GFCE) Foundation, we submit the following contribution to the Third 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 highlight the importance of multistakeholder participation and cooperation in combatting cybercrime, and further elaborate on 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 international Convention.

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.

The GFCE is a broad coalition of over 170 Members and Partners, representing a unique multistakeholder community that includes 65 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 such as the Organization of American States (OAS), AFRIPOL, INTERPOL, the African Union (AU), the Council of Europe, the Organization for Security and Cooperation in Europe (OSCE), and the World Bank. The GFCE also counts industry bodies and private sector actors, civil society, technical organizations and academia amongst its Partners.

As has been well documented, combatting cybercrime is a multidisciplinary activity that requires the cooperation of various stakeholders operating across policy and operational domains. A multistakeholder approach is vital to addressing the transnational challenges of malicious use of ICTs and to protecting and empowering users of these technologies. The GFCE is therefore encouraged to see modalities for the inclusion and participation of non-state stakeholders in the Ad-Hoc Committee.

The GFCE's unique position and key role in facilitating and coordinating capacity building efforts is made possible by its neutrality, community-driven, and action-oriented approach. Over the course of seven years, this community has established and maintained a flexible and diverse ecosystem geared towards the needs of its members and that mobilizes multistakeholder engagement by design.

The GFCE Working Group 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.

Given the GFCE's standing and its established multistakeholder network, we strongly encourage the UN and all Member States 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. Stronger cooperation with platforms such as the GFCE can also be beneficial for the UN and Member States in accessing requisite support for capacity building and technical assistance for addressing cybercrime.

In negotiating the Convention, the GFCE calls on States to fully take account of existing international and regional frameworks pertaining to cybercrime with the aim of encouraging complementarity and further developing understanding on how existing measures and initiatives can be leveraged to mitigate the scope and impact of cybercrime.

Capacity building is a fluid concept requiring a flexible approach that fully takes account of diverse needs and challenges across the design and delivery of initiatives. In this respect, it would be advisable for the prospective Convention not to be too prescriptive on the delivery of capacity building. International organizations such as UNODC and INTERPOL are already playing an important role in the coordination and facilitation of technical assistance and capacity building. Yet, 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 is of the view that defining overly specific roles for relevant 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 calls on the UN to encourage all stakeholders to cooperate and conduct capacity building on the basis of clearly defined principles. For example, the effective participation and involvement of all stakeholders in capacity building is one of the core principles of the GFCE's Global Agenda for Cyber Capacity Building, endorsed by all GFCE Members and Partners.

In this regard, the GFCE also recognizes that the prevention and control of cybercrime and measures to enhance cybersecurity are mutually reinforcing. An effective criminal justice response to offences against ICT thus reinforces cybersecurity. It is therefore critical that there is a greater understanding of how international frameworks and policy discussions on combatting cybercrime and promoting responsible state behaviour in the use of ICTs may be better leveraged for coherent responses at all levels. Though separate and distinct subject matter, lessons and parallels can also be drawn from the UN First Committee, in particular the principles for capacity building as outlined in the final report of the OEWG on ICTs in the context of international security.

In addition, capacity building requires trust between donors, implementers and beneficiary communities to ensure sustainable, equitable and long-term impact. The most effective way of building this trust is through encouraging partnerships that ensure meaningful participation of those that require capacity building throughout the entire lifecycle.

GFCE is increasingly committed and well-positioned to support demand-driven and needs-based delivery of capacity building and analysis. Through the AU-GFCE program, representatives of over 30 AU Member States and 25 multi-national African organizations, associations, and Regional Economic Communities (RECs) have joined forces to map capacity building needs, expertise and priorities across the continent. After extensive consultation with various cyberspace communities and stakeholders, the GFCE is also in the process of establishing a capacity building hub in the Pacific and plans to establish similar coordination points in South-East Asia and in the Americas alongside international partners such as the Organization of American States.

Similarly, through support provided to the Women in International Security and Cyberspace Fellowship program and the establishment of a Women in Cyber Capacity Building Network, the GFCE is also contributing to efforts aimed at ensuring capacity building is reflective of gender considerations and improving understanding on how the meaningful participation of women in discussions concerning cyberspace can improve policy responses to cybercrime.

With regard to existing and planned capacity building activities, the GFCE calls on States to commit to providing transparent information on measures taken to address cybercrime through capacity building, including the challenges they have faced with respect to the establishment and implementation of capacity building efforts. Divergences in information regarding levels of development and implementation of capacity building measures, particularly at the regional level, can have a negative effect on the ability and expectations of stakeholders. Better understanding of policy and practical measures undertaken by States and organizations alike is therefore essential.

To support this, the UN could encourage States to share such information, referencing repositories such as the GFCE's Cybil Portal as a good starting point for setting a baseline for mapping cybercrime capacity building activities globally. As a unique knowledge hub for cyber capacity building, the Cybil Portal is fast becoming a comprehensive source of basic project information, with information on over 170 projects and 75 resources on cybercrime alone in its repository.

In conclusion, many States, law enforcement agencies and criminal justice authorities still lack the technical, institutional and policy capabilities to respond to malicious cyber events, cooperate internationally, and fully participate in the many international debates that are shaping the future of cybercrime prevention and response. A substantial answer to both preparing countries and organizations to deal with the threats posed by cybercrime is capacity building. Yet, cyber capacity building remains underprioritized and underfunded.

The Ad-Hoc Committee process can have a positive effect for encouraging States and non-state actors alike to share their positions on capacity building. However, there is already an urgent need to ensure that all stakeholders – especially States – have the necessary capacity to effectively participate in such processes and begin to implement and enforce measures agreed in institutional fora, including those related to cybercrime. The GFCE therefore harbors hope that this process can also be a catalyst for increased transparency and unlocking of much-needed resources for capacity building.