Fourth intersessional consultation of the Ad Hoc Committee

Vienna, 6 and 7 March 2023

Presentation Global Forum on Cyber Expertise – Tereza Horejsova

Intro

- Through my intervention, I will **highlight the importance of multistakeholder participation and cooperation in the response to cybercrime**,
- from the perspective that partnerships with non-governmental stakeholders are key to ensure effective technical assistance.
- I will elaborate on how the **Global Forum on Cyber Expertise 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
- 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.
- By elaborating on the GFCE ecosystem, I will indicate **how GFCE mechanisms and tools contribute to a better understanding of countries' needs and priorities, support a tailored, targeted approach for technical assistance and to coordinated, effective capacity building efforts in general.**

Using GFCE's platform as an example of how stakeholders are working together

- For those who are less familiar, the GFCE is a neutral multistakeholder community of over 180 members and partners including states, international and regional organizations, the 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 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**.
- To achieve this, it has been crucial to facilitate connections in the Community and promote collaboration.
- I'd like to highlight a few of GFCE's mechanisms and tools that it has developed to make this possible– the working groups, research agenda, the Cybil Portal and the Clearing House, as well as its regional focus.

Working Groups

- The GFCE's multistakeholder community come together to share, shape and form knowledge on specific issues in thematic **Working Groups**.

- 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.

Research Agenda

- Within the Working Groups, the community **identifies knowledge gaps and prioritizes them**, resulting in the development of a bi-annual Global Capacity Building Research Agenda.

- Through the GFCE's Research Agenda, **knowledge gaps on types, causes and effects of offences covered by the future Convention can also be proposed**, engaging the academic community to support informed practical strategies and solutions by providing data and analysis.

Cybil Portal

- In previous years, focus has been placed also on **improving existing knowledge on the supply side of cyber capacity building**

- As we have found that a **lack of information on existing efforts – or similarly a lack in understanding of needs – has been detrimental to the overall goal of improving cyber capacity**

- As such, another important tool that the GFCE Community has developed is the **Cybil Portal** – **a global, open and free knowledge repository** with information on over 800 cyber capacity projects, and over 300 tools and resources.

- Cybil contributes to stronger global cyber security and cybercrime capacity by helping capacity building projects be more effective – through accessibility on information and improving transparency.

The GFCE's Match Making / Clearing House function

- This matchmaking role refers to **recipient countries identifying themselves where support is needed based on their specific situation, and the GFCE putting those actors in touch with members and partners that can provide targeted capacity building support**.

- The GFCE provides a space for **international implementing partners to connect with the recipient 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 with the international donor community to support the rollout of the national cybercrime awareness program.

- The CH mechanism foresees a built-in strong **local stakeholder involvement** in all the stages of developing and implementing the capacity building response which ensures local **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.

- **Through the regional focus and accessible Clearing House function, particular attention is given to developing countries**

Further examples of demand-driven initiatives addressing cybercrime

- GFCE is increasingly committed and well-positioned to **support demand-driven and needs-based delivery of capacity building and analysis**.

- As an example, 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.

- **Combatting cybercrime** and **child online protection** phave been identified as priority areas by the ACE community, and converted into Knowledge Modules, in cooperation with the DiploFoundation.

- 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.

Conclusion

- While acknowledging that negotiations within the context of the UN and AHC are multilateral and state-led processes, we would encourage 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 can 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.