About the GFCE

Global Forum on Cyber Expertise

Introduction

The **Global Forum on Cyber Expertise (GFCE)** was launched at the Global Conference on Cyber Space in The Hague based on this vision: everyone should be able to fully reap the benefits of ICT through a free, open, and secure digital world. It was anticipated that the GFCE would develop into a global, informal and coordinating platform for cyber capacity building. The GFCE was tasked with a clear mission ***to strengthen cyber capacity and expertise globally by being a pragmatic, action-oriented and flexible platform for international cooperation***. The unique structure of the GFCE as a bottom-up, neutral and apolitical forum provides an excellent opportunity for multi-stakeholders to exchange best practices and expertise on cyber capacity building.

The GFCE's mission can be summarized into three strategic objectives:

- ***Coordination*:** Avoid the duplication of efforts and blind spots by coordinating projects;
- ***Knowledge sharing*:** Improve efficiency and effectiveness in the delivery of cyber capacity programs by sharing knowledge and expertise;
- ***Clearing house*:** Fill capacity gaps and support the capacity building needs of countries.

Developments of the GFCE over the years

In the first years of the GFCE, the focus was on building a strong GFCE network (now with over a 100 active Members and Partners) and awareness raising regarding existing Capacity Building Programs. In 2017, the GFCE positioned itself as the coordinating platform for cyber capacity building by developing the Global Agenda for Cyber Capacity Building. After a year of conducting extensive consultations and research, the entire GFCE community endorsed the **Delhi Communiqué on a GFCE Global Agenda for Cyber Capacity Building**.

The Delhi Communiqué prioritizes five themes in cyber capacity building and calls for action to jointly strengthen global cyber capacities. Throughout 2018-2019, the structure of the GFCE has evolved to support the ecosystem. A key element of this GFCE ecosystem are the Working Groups. The GFCE Working Groups encourage the multi-stakeholder dialogue on the implementation of cyber capacity building: bringing together needs, resources and expertise. Many GFCE Members and Partners work together on broader themes and specific topics on cyber capacity building as identified in the Delhi Communiqué:

- Cyber Security Policy & Strategy
- Cyber Incident Management & Critical Information Protection
- Cybercrime
- Cyber Security Culture & Skills
- Cyber Security Standards

To support the efforts of the GFCE Working Groups, there are cross-cutting groups that aim to tie the Working Groups together under the objectives of the GFCE. These groups include the GFCE Advisory Board, the Cybil knowledge portal group, the clearing house group and the private sector group; which have a key role in supporting the cyber capacity building ecosystem.

About the GFCE

Global Forum on Cyber Expertise

Achievements in supporting the Cyber Capacity Building ecosystem

The Global Forum on Cyber Expertise (GFCE) was established to strengthen cyber capacity building and coordinate existing international efforts more effectively. The focus of the GFCE in 2019 and 2020 is to further ***strengthen an ecosystem for international cooperation on cyber capacity building***. Key elements of this ecosystem are the GFCE Working Groups, the establishment of the CCB knowledge portal, and a GFCE clearing house mechanism.

- **GFCE Working Groups** – the Working Groups aim to strengthen international cooperation / coordination on their respective theme by developing a common focus, enabling efficient use of available resources, and avoiding duplication of efforts. The Working Groups focus on identifying who's doing what (coordination), what useful tools are already out there (knowledge sharing), and how the Working Group can help a member with a request for support (clearing house).
- **Cybil - CCB knowledge portal** - a unique source of information on tools, publications, overview of activities on cyber capacity building globally, and the GFCE Working Group outcomes. To underline the global character of Cybil, the Working Groups have to approve the tools and publications that are uploaded on Cybil through a silent procedure. While most of the content on Cybil is currently gathered through the GFCE community, the Cybil Advisory Board (knowledge partners) are amongst others actively promoting Cybil in their networks to gather ideas and input from the global community.
- **GFCE clearing house mechanism** - effectively matching country, private sector and civil society (resources and expertise) that can provide key capacity building services with countries (beneficiaries) that require assistance in one or more aspects of cyber capacity building. With an effective global clearing house mechanism, the GFCE improves efficiency on a global level in the delivery of capacity building programs by avoiding duplications and blind spots.

GFCE Working Group on Cyber Security Policy and Strategy

The theme Cyber Security Policy and Strategy can be seen as the foundation of the other identified themes in the Delhi Communiqué as developing a National Cybersecurity Strategy is the first step to tackle other cyber issues. The aim of the group is thus to help countries and other stakeholders improve their policy and strategy making capacity. Recognizing the importance of the international cyber CBMs and Norms efforts, the Working Group formed a new ***Task Force on CBMs and Norms Implementation & Cyber Diplomacy*** at the IGF in 2018.

The Task Force is unique as it focuses on practical cyber capacity building with regards to CBMs, norms implementation and cyber diplomacy and aims to empower countries with the necessary capacity to engage with such discussions on the international level. In 2019, the Task Force mapped existing CBMs and norms, and identified key stakeholders, actors, and events in this space. The Task Force has also mapped over 50 cyber capacity building projects and developed a repository of relevant tools and publications on Cybil, the CCB Knowledge Portal. During the GFCE Annual Meeting 2019 in Addis Ababa, the Task Force organized a workshop to give participants a greater understanding of international discussions on cybersecurity and to discuss what capacity is needed to implement specific norms/CBMs. At this stage, the Task Force seeks to bridge countries with the complex international cyber discussions and explore ways to support the practical implementation of the outcomes of such discussions.

For more information on the Task Force, please contact the GFCE Secretariat at contact@thegfce.org.