Background Paper of the Global Forum on Cyber Expertise (GFCE):

Submission on the 15th Annual Meeting of the Internet Governance Forum

22 April 2020

What is the GFCE

The Global Forum on Cyber Expertise (GFCE) is a multi-stakeholder platform that aims to strengthen cyber capacity and expertise globally through international collaboration. Established in 2015, the GFCE has steadily grown into the leading international platform for cooperation on cyber capacity building.

We must strive towards an open, free, peaceful and secure digital world if we are to fully reap the benefits of ICT. This can only happen when all actors work in tandem to achieve common objectives. The GFCE is an action-oriented, flexible and consultative forum valued by its members for its multi-stakeholder approach to cyber capacity building that allows for the exchange of best practices and coordination of efforts in the cyber capacity building field.

Since its inception the GFCE has been an umbrella organization for governments, private sector actors, technical and academic organizations to engage in dialogue and have an impact at local, regional and international levels by connecting needs, resources, expertise and making practical knowledge available to the global community.

Who is the GFCE

The idea of a platform to share cyber expertise for global cyber capacity building was born from discussions at the 2015 Global Conference in Cyber Space (GCCS) in the Hague, hosted by the Government of The Netherlands.

Since then the GFCE has grown from 42 initial supporters into an organization with over 115 members and partners from all regions of the world. The GFCE aims to have a strong physical as well as online presence, having held over 50 events in the global North and South and been an incubator for 21 global and regional initiatives.

Participation in the GFCE is as diverse as its membership, with those involved performing functions at all levels of their respective organization or country. This spans from working level to those in key positions for decision making. Participation in the GFCE is voluntary and all members are responsible for the functioning of the GFCE and initiatives – this means that all members and partners collaborate and work towards the development of the platform on an equal footing.

The GFCE Foundation Board was installed upon establishment of the GFCE Foundation in December 2019. With Mr. Christopher Painter as President, supported by Ms. Inge Bryan as Secretary and Mr. Olaf Kolkman as Treasurer, the Foundation Board is responsible for offering strategic guidance for the GFCE community and Secretariat, establishing continuity through outreach and fundraising, and providing a visible point of communication for the Foundation.

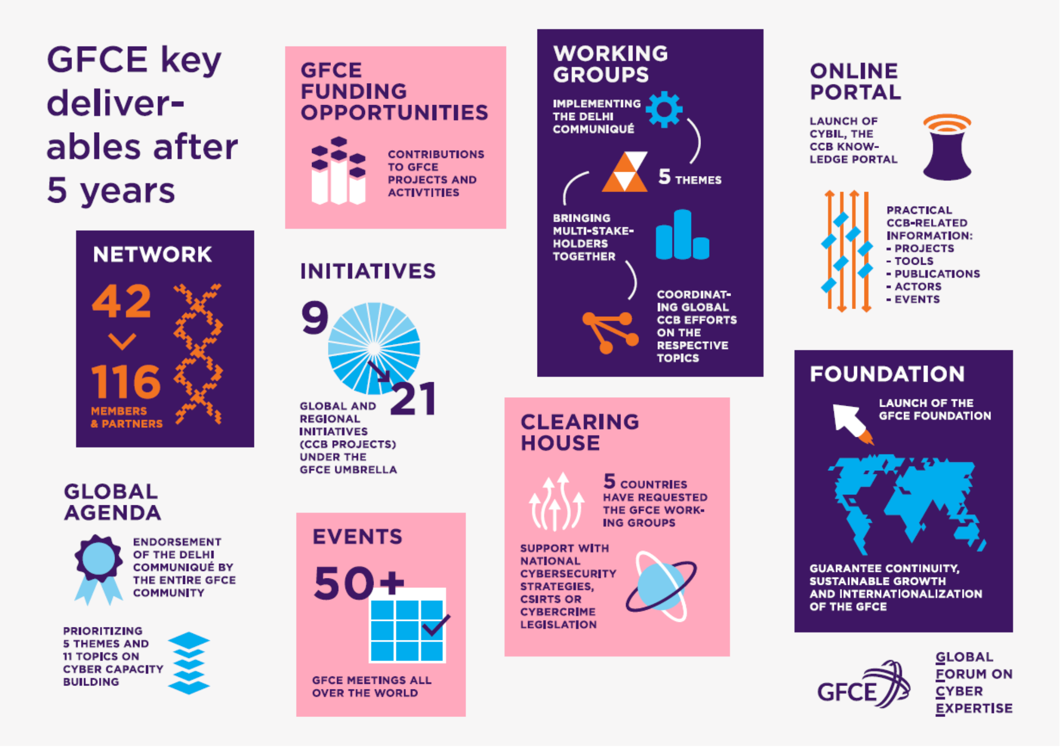
To further promote active involvement of civil society, academia and the technical community, the first GFCE Advisory Board was established in 2016. The main role of the GFCE Advisory Board is to provide advice on the overall direction of the GFCE as well as giving substantive input and recommendations to the GFCE Working Groups.

The GFCE is also supported by a Secretariat, which provides logistical and administrative functions as well as collecting and coordinating the sharing of relevant information and analysis on projects and initiatives for GFCE members.

Further information on the GFCE and its members and partners can be found on the website www.thegfce.org or in the GFCE Global Cyber Expertise Magazine, accessible on the GFCE website. The 7th version of the GFCE Magazine is a joint initiative by the African Union, the European Union, the Organization of American States and the GFCE, aiming to provide cyber policymakers and stakeholders insight on cyber capacity building projects, policies and developments globally.

Charting the 5-year growth of the GFCE

The year 2020 is a special milestone for the GFCE as it celebrates its fifth anniversary in April and is now officially established as a GFCE Foundation. Committed to its mission to strengthen cyber capacity and expertise globally through international collaboration, the GFCE has met many achievements during these five years, including building a strong foundation and community to



GFCE key deliver-ables after 5 years
NETWORK
42
116
MEMBERS & PARTNERS
GFCE FUNDING OPPORTUNITIES
CONTRIBUTIONS TO GFCE PROJECTS AND ACTIVTITIES
INITIATIVES
9
21
GLOBAL AND REGIONAL INITIATIVES (CCB PROJECTS) UNDER THE GFCE UMBRELLA
WORKING GROUPS
IMPLEMENTING THE DELHI COMMUNIQUÉ
5 THEMES
BRINGING MULTI-STAKE-HOLDERS TOGETHER
COORDINAT-ING GLOBAL CCB EFFORTS ON THE RESPECTIVE TOPICS
ONLINE PORTAL
LAUNCH OF CYBIL, THE CCB KNOW-LEDGE PORTAL
PRACTICAL CCB-RELATED INFORMATION:
- PROJECTS
- TOOLS
- PUBLICATIONS
- ACTORS
- EVENTS
GLOBAL AGENDA
ENDORSEMENT OF THE DELHI COMMUNIQUÉ BY THE ENTIRE GFCE COMMUNITY
PRIORITIZING 5 THEMES AND 11 TOPICS ON CYBER CAPACITY BUILDING
EVENTS
50+
GFCE MEETINGS ALL OVER THE WORLD
CLEARING HOUSE
5 COUNTRIES HAVE REQUESTED THE GFCE WORK-ING GROUPS
SUPPORT WITH NATIONAL CYBERSECURITY STRATEGIES, CSIRTS OR CYBERCRIME LEGISLATION
FOUNDATION
LAUNCH OF THE GFCE FOUNDATION
GUARANTEE CONTINUITY, SUSTAINABLE GROWTH AND INTERNATIONALIZATION OF THE GFCE
GFCE
GLOBAL FORUM ON CYBER EXPERTISE

support cyber capacity building globally and position itself as the international coordinating platform on cyber capacity building.

GFCE Initiatives

In the first two years, the GFCE was organized around regional and global initiatives. As a bottom-up platform, members and partners could choose what they wanted to initiate, collaborate on, and where to provide specific expertise. By sharing best practices and lessons learned, the GFCE aimed to improve cyber capacity building efficiency and effectiveness.

Setting the Global Agenda and the GFCE Working Groups

One of the turning points for the GFCE was the 2017 GCCS in New Delhi, where the GFCE put forth and received support for the Delhi Communiqué on a Global Agenda for Cyber Capacity Building. This provided the necessary political impulse for the recognition of the importance of cyber capacity building, putting CCB coordination of efforts on the map. Furthermore, developing a Global Agenda was crucial in order to determine priorities and methods for implementation in 2018 and beyond.

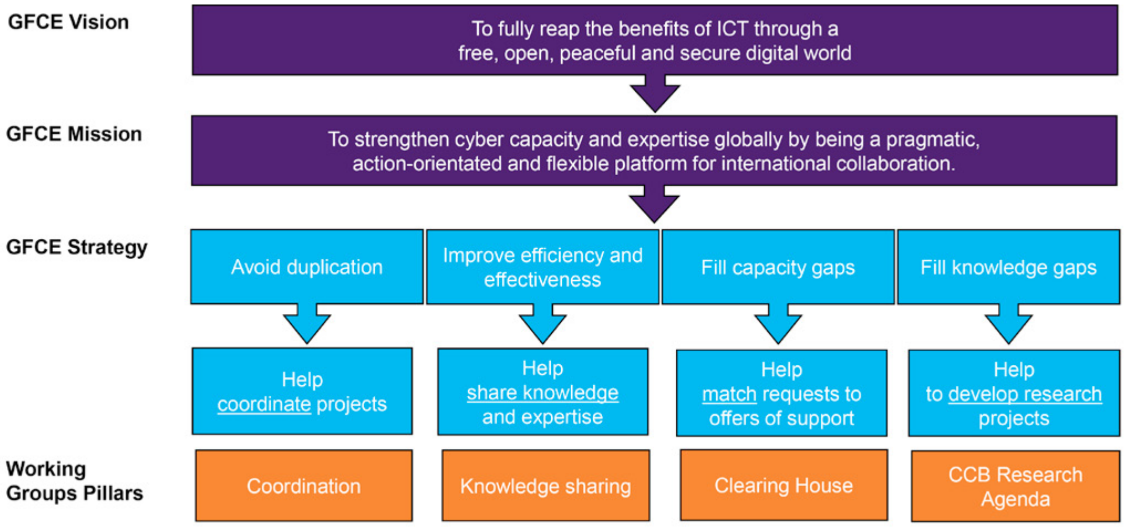
By developing the Agenda, the GFCE effectively shifted its focus in 2017 to position itself as the platform for exchanging cyber expertise and coordinating global cyber capacity building efforts. Building on the global good practices identified through GFCE initiatives, the Global Agenda prioritized five themes and eleven topics, calling for action to jointly strengthen cyber capacities globally. The entire GFCE community endorsed the Delhi Communiqué, which was essential not only to coordinate global efforts but also to encourage multi-stakeholder dialogue on its implementation.

As a first step towards concrete action on the implementation of the Agenda, a new structure in the GFCE was established – the GFCE Working Groups. In the Working Groups, Members and Partners work together and collaborate on topics that fall under the Group's broad theme, as prioritized in the Delhi Communiqué. These themes are: Cyber Security Policy and Strategy, Cyber Incident Management and Critical Infrastructure Protection, Cybercrime, Cyber Security Culture and Skills, Cyber Security Standards.

Today, the Working Groups delivers the GFCE's mission by being the engine and lifeforce of the GFCE, involving over 85% of the Community. For coherence and synergy, the work and common deliverables of all Working Groups are divided across the same four pillars:

1. Coordination
2. Knowledge sharing
3. Clearing House Mechanism
4. Cyber Capacity Building Research Agenda

Each of the pillars have been derived from the GFCE's overall strategy as illustrated below.



GFCE Vision

To fully reap the benefits of ICT through a free, open, peaceful and secure digital world

GFCE Mission

To strengthen cyber capacity and expertise globally by being a pragmatic, action-orientated and flexible platform for international collaboration.

GFCE Strategy

Avoid duplication → Help coordinate projects

Improve efficiency and effectiveness → Help share knowledge and expertise

Fill capacity gaps → Help match requests to offers of support

Fill knowledge gaps → Help to develop research projects

Working Groups Pillars

Coordination | Knowledge sharing | Clearing House | CCB Research Agenda

Cybil Knowledge Portal

This globally owned one-stop knowledge hub brings together knowledge on international cyber capacity building. It is a unique source of information on tools, publications, overview of activities on cyber capacity building globally, upcoming events, and the GFCE Working Group outcomes. In October 2019, the GFCE launched the Cybil Knowledge Portal together with knowledge partners that form the Portal Group - NUPI, GCSCC, FIRST, DiploFoundation and ASPI. Since its launch, new features of Cybil include an events calendar with information on upcoming cyber capacity building conferences, workshops and meetings around the world. As of March 2020, Cybil contains 500 projects, 72 tools, 74 publications, 421 actors and 39 upcoming events. The content is identified and updated by the GFCE community through the GFCE Working Groups.

Clearing House

Recognizing that cyber capacity building can never be a one-size-fits-all model and that tailored assistance to local contexts is a determinant of successful capacity building projects, the GFCE seeks to be a capacity building clearing house. Through the GFCE Working Groups, the GFCE plays a ‘match-making’ role – effectively matching countries that have specific CCB needs with country, private sector and civil society donors and implementers that can provide key capacity building services.

Cyber Capacity Building Research Agenda

In discussing the challenges faced by the GFCE community, it became increasingly clear that knowledge gaps existed and the GFCE could potentially address these gaps. To help the capacity building community design and run effective projects, a new pillar of the GFCE Working Groups was introduced in 2020. Through the Working Groups, knowledge gaps and research that would be useful and that may help the community achieve their strategic and operational goals are being identified.

The GFCE is collecting and prioritizing these research needs into a Global Cyber Capacity Building Research Agenda. This also responds to the call of the GFCE Community for a flexible mechanism that would help them identify common research requirements and generate targeted research relevant to ongoing GFCE work and Member's activities. The Advisory Board has taken the lead on developing this idea into a clear process, with the formation of the GFCE Research Committee as the first actionable step.

GFCE Foundation

In December 2019, the GFCE embarked on its transition into an independent, not-for-profit GFCE Foundation. With an international Foundation Board, the GFCE Foundation becomes a vehicle that enables sustainable growth, allowing amongst other things for it to take a more strategic outlook in the long term as it begins charting a new course. The strategic direction will be informed by the GFCE community, with Members and Partners asked to provide input on the GFCE's way forward.

The Future of the GFCE & Cyber Capacity Building: Looking Ahead to 2022

The future is bright for the cyber capacity building community. As the GFCE looks ahead to 2022 it aims to further strengthen the GFCE ecosystem by improving processes, expanding its work methods and the community whilst encouraging active engagement, establishing a truly global and regional presence through organizing more meetings around the world.

Today, the GFCE is the only platform that coordinates global cyber capacity building, reducing the duplication of efforts in the cyber capacity building ecosystem while maximizing available expertise and resources. Key to the successes of the GFCE as a global coordinating platform on CCB is the endorsement of governments around the world.

The importance of sustainable cyber capacity building efforts was acknowledged most recently in the United Nations First Committee by the Open-Ended Working Group, which noted in the pre-draft of its report[1] that sustainable capacity building efforts are an enabler for stakeholders in increasing security and stability globally and empower them to fully participate in the global normative framework. At the multilateral level, this has significant impact on the promotion of adherence to international law and the implementation of norms of responsible State behavior, and for building trust between and within States. The GFCE will continue to engage with such processes to better define how it can support efforts at the multilateral level to facilitate and coordinate on cyber capacity building.

Another major factor is the ability of the GFCE community to continue to actively share expertise and voice their capacity needs. Input from the community provides much-needed perspective on crucial aspects of the future of the GFCE platform, for instance on the Cybil Knowledge Portal, the GFCE Clearing House Mechanism and Global CCB Research Agenda.

[1] United Nations Open-ended Working Group on developments in the field of information and telecommunications in the context of international security (OEWG), Pre-draft to its Report, 16 March 2020

Together with the GFCE Foundation Board, the GFCE Secretariat looks forward to driving momentum for realizing the GFCE's vision and mission by encouraging active engagement of the GFCE community whilst demonstrating its added value to those outside the community. Whilst the

GFCE is a multi-stakeholder organization made up of representatives from governments, private sectors actors, technical and academic institutions, it goes without saying that continued engagement with diverse stakeholder groups is key to the development of cyber capacity building.

Involving multiple stakeholders in collaboration on CCB is crucial as there are many different facets to consider that require different expertise – for instance, institution building, establishing computer emergency response teams (CERTs) or developing national strategy and encouraging adoption.

A fundamental characteristic of capacity building is the need for trust between stakeholders. The GFCE believes that it can have added value in the area of CCB by increasing trust and legitimacy – this begins with generating dialogue and building relationships, thereby promoting understanding between actors in the process.

Furthermore, staying actively committed to its mission, the GFCE recognizes that strong cyber capacity and exchanging of expertise is necessary not just for achieving digital security but also for making progress on economic and social development. This is true wherever such dialogue takes place, though the outcomes are stronger and have greater impact if they are inclusive of the needs and perspectives of all stakeholders from the outset.

Civil society engagement can lead to better informed and evidence-based policy outcomes, leading to more effective implementation of the cyber policies. In its implementation, cybersecurity policy affects stakeholders across a community. Bringing this expertise into any cybersecurity discussion or policymaking process can help get a more accurate and evidence-based picture of the cybersecurity landscape, the possible implications of different policies being considered, and can build confidence and trust in the policy itself as well as with other stakeholders involved in its implementation. Stakeholders who have been involved in the development of a policy or strategy will have a stronger understanding of it and what is required from them making implementation efforts more effective.[2]

The GFCE therefore hopes to improve regional coordination by engaging with stakeholders on matters of core important to its values and mission. This involves more widespread and increased engagement in the diverse consultative multi-stakeholder fora and processes across the governance ecosystems. For the GFCE, this also means that it continues to strengthen its own platform and looks to establish a regional presence in different continents, stepping up GFCE regional coordination meetings began in 2020.[3] Ultimately, as a community-driven platform, the GFCE will to continue to be open and flexible to new ideas and encourage the community to be critical, keeping cyber capacity building at the forefront of the global agenda.

[2] Daniela Schnidrig & Klee Aiken, *Stakeholder engagement in cyber capacity building – lessons learned after 5 years of the GFCE*, GFCE Magazine 7th Ed. (2020)

[3] Regional Meetings are planned for the Americas, Africa and Southeast Asia and have already been held for Europe and Pacific in 2020. More information on the Pacific Regional Meeting can in the article "GFCE meets the Pacific".