GFCE Roadmap

“Working towards a global cyber capacity building agenda”

1. Introduction

The opportunity for economic and human development provided by cyberspace capabilities and the impressive growth of cyberspace activities over the last few decades is undisputed. Globally, societies have become increasingly digitized. It is therefore more and more important for states, international organizations, private companies and civil society to put the potential of cyber capabilities at the service of development, in order to address the threats posed by malicious cyber activities and to promote secure digital services and infrastructure.

Resilient systems which need to guarantee our access to the internet is free, open and secure can only exist when all parties who have a stake in the cyber domain undertake collective efforts. This is exactly the reason why the Global Forum on Cyber Expertise (GFCE) at the Global Conference on Cyberspace (GCCS) in The Hague was launched in 2015: to strengthen cyber capacity and expertise globally, while upholding the values of an internet that is free, open and secure.

1.1 Purpose and outline of the roadmap

With this document, the GFCE outlines a process for the coming year. The roadmap sets out the first concrete steps towards a more long term engagement through the development of a “global cyber capacity building agenda” and “global good practices”. The agenda and good practices will form the basis for a long term strategy for the GFCE. Evidently, this process needs to be owned by all GFCE members, jointly striving towards a shared agenda.

In November 2017, the next GCCS is tentatively planned to take place, hosted by India. The GCCS2017 could provide momentum for the GFCE to present itself as a worldwide coordinating platform and to give a political impulse to the importance of cyber capacity building. Not only because the GFCE was launched at the GCCS2015 but also as the GCCS rallies a large group of cyber stakeholders from various backgrounds.

Note has to be made that deliverables which are put forward in the roadmap are required for the GFCE to define a more long term strategy, irrespectively of the GCCS2017. But if possible, the GFCE could now leverage the GCCS2017 to share its future cyber capacity building agenda with the rest of the world. Therefore, the GFCE has the ambition to finalize the process of development of an agenda for cyber capacity building and the global good practices by the time of the GCCS2017.

Since defining a long term strategy for the GFCE is a next step beyond and building on the deliverables as described in the roadmap, it is not considered a deliverable of the Roadmap.

Note has to be made that while following this roadmap, the GFCE needs to remain flexible to rapidly adjust to changes.

The GFCE roadmap proposed here has been prepared in accordance with the GFCE members and following the input from the GFCE Advisory Board.

2. GFCE Vision and Mission

The GFCE is a global platform for primary stakeholders to exchange good practices and expertise on cyber capacity building. The objective of the GFCE is to identify successful policies, practices and ideas, and to multiply these on a global level. Under the umbrella of the GFCE initiatives to build cyber capacity are being developed. GFCE events offer a one-stop-shop for a continuous policy discussion and for finding partners and/or resources for cyber capacity building activities. By matching demand and supply, the GFCE functions as clearing house for its members.

The initial themes for capacity and expertise building within the GFCE are strengthening cyber security, fighting cybercrime, protect online data and support electronic (e-) governance.

3. Added value and next steps

3.1 The added value of the GFCE

During summer 2016, the GFCE Secretariat held a number of consultations with the GFCE members in order to understand what the members consider the added value of the objectives behind the GFCE and to be in a better position to respond to their needs and challenges. Four areas were identified, which support the overall GFCE mission.

3.1.1 The first identified area in which the GFCE has a clear added value is as a ***knowledge repository and a place to exchange ideas on good practices***. The GFCE brings together demand and supply of cyber knowledge and expertise. The GFCE will recommend expertise inside and outside the forum (while keeping in mind contextual specifics), thereby having the potential to unlock not only existing knowledge but also to develop new ideas.

3.1.2 The second area focuses on the role of the GFCE as a ***coordination mechanism***. The GFCE contributes to a better overview of existing and planned capacity building initiatives in order to avoid duplication, minimize conflict of actions, and wherever possible promote synergies and cooperation

among (regional) stakeholders. The GFCE could also be used by donors of cyber capacity projects to coordinate resources.

3.1.3 Thirdly, the GFCE could be considered a ***clearing house*** that helps match members looking to share ideas and good practices with members looking to implement projects or host projects in their respective countries..

3.1.4 Lastly, although the GFCE is a non-political forum, it is committed to a cyberspace which is ***free, open and secure***. The efforts undertaken within the framework of the GFCE will be consistent with international law, in particular the Charter of the United Nations, and respect the Universal Declaration of Human Rights, the International Covenant on Civil and Political Rights and the UN Guiding Principles on Business and Human Rights, where appropriate.

3.2 Taking stock and raising the level of ambition

After one year, the GFCE will be able to reflect on the gaps which need to be addressed and the required actions to lock its position as a coordination platform for cyber capacity building.

Looking back at a glance, the first steps towards a knowledge repository have been made through the cybersecurity capacity portal in partnership with the Global Cyber Security Capacity Centre (GCSCC); the Global Cyber Expertise Magazine has been launched, the number of (strategic) members has increased to a total of 55 and the 12 capacity building initiatives organized several events and expert meetings throughout the year.

In the second year of its existence, the GFCE will take a look at the future; where do we want to go and what would be required to get there. The GFCE will raise the level of ambition by striving towards the following deliverables to strengthen its added value;

1. A global cyber capacity building agenda which identifies future priorities for cyber capacity building. This brings together the role of the GFCE as a knowledge sharing platform, as well as a coordination mechanism.
2. Global good practices in support of the GFCE as an actionable forum.

Building on what has already been done in the four areas as identified above (added value), the following paragraphs will set out the steps that the GFCE needs to take to be able to deliver a global agenda and good practices.

3.2.1 Leveraging the coordination mechanism of the GFCE and linking it to the knowledge repository: Global cyber capacity building agenda

As stated in the GFCE Framework document, the GFCE aims to organize several high level meetings to "provide the opportunity to discuss and (re)formulate requirements as well as best practices on cyber capacity building in the identified thematic areas. This will promote a continuous policy discussion about

ways and means to respond to emerging challenges in the cyber domain, while preserving each member's internal decision making processes on implementation of specific measures."

In the second year since its launch, the GFCE aims to organize such a high level meeting. This discussion is foreseen to bring together a high level delegation from the various members of the GFCE. The GCCS2017 would provide an excellent platform to do this.

The entry point for this discussion would be a shared agenda on an agreed ambition (for example: every country has a cybersecurity strategy; or substantially increasing the number of CERTs worldwide). Which elements should actually become those future priorities will be based on a process within the GFCE community. In collaboration with its members and partners, the GFCE will then steer the development of an internationally coordinated response to cyber capacity building.

This process towards this capacity building agenda will consist of continuous dialogues amongst the members through various platforms such as the Annual Meeting; break out groups and virtual meetings

The discussions will need to be fed by not only the work done and experiences gathered under the initiatives but also by the information collected as part of the knowledge sharing efforts. The activities related to the latter will be expanded by several research papers and a research initiative. In sum up, the following (foreseen) sources can be used;

1. Analysis of existing capacity building initiatives under the GFCE
2. Analysis of existing capacity building initiatives worldwide (based on the cybersecurity capacity portal in partnership with the GCSCC)
3. Analysis provided by the newly established GFCE Research Initiative
4. Outcomes of the GFCE initiatives

By using the different resources, the GFCE strives to loop the different strands (initiatives and knowledge repository) back into the global agenda.

3.2.2 Syncing the outcomes of the initiatives: Global good practices

Through the GFCE, stakeholders have the advantage to learn from the experience of others. Capacity building initiatives in the making can utilize and adapt good practices gained from the experience in other GFCE initiatives or the development cooperation community at large. The GFCE can help to identify these good practices based on the information collected from the GFCE community. Once there is consensus that a good practice has proven itself under various circumstances, a list of commonly agreed good practices can be established. Good practices are not intended as a one-size fits all model. They are merely recommendations, providing a selection of measures as to how stakeholders can improve and strengthen their cyber activities. Needless to say, the good practices should be adapted to specific (local) circumstances based on the needs.

To prepare the development of the global good practices on cyber capacities each ongoing initiative under the GFCE will be asked to **distill three good practices** and the tools required to implement these good practices. Good practices will be based on operational components of the initiatives which are translated to policy setting.

The information can be drawn not only from the outcomes of the GFCE initiatives but also from the experience of the development community and other widely recognized sources such as regional and international organizations. They will take into account the lessons learned, success factors and equally important; less successful actions.

During the **GFCE Annual Meeting,** the initiative leads will be asked to present their preliminary good practices to the members for further interactive discussion. In smaller groups, these good practices will be discussed and analyzed with the aim to possibly present them during the GCCS. To support this process, the GFCE Secretariat will be sharing some suggestions in advance as how to distill these good practices from the initiatives.

During the discussions and in the **months up to the GCCS**, potential overlap and synergies could be signaled by the GFCE members, the Advisory Board and the Secretariat. The GFCE Secretariat could connect the initiatives concerned, so they can jointly continue working on the (overarching) good practices. The good practices will be based on the experiences and information collected so far but could evolve over time, due to the ever changing cyber landscape.

As for the global cyber capacity building agenda, the GCCS2017 would provide an excellent platform to officially highlight the good practices.

3.2.3 New initiatives: filling the gaps

To come up with a broad list of global good practices which represents the mission and working areas of the GFCE, it is important to revisit the current GFCE initiatives and analyze whether there are any gaps.

Members indicated that the number of initiatives could be expanded to deliver concrete outcomes and stimulate knowledge sharing. There is potential for new initiatives on topics of mutual interest on all four GFCE themes (cybersecurity, cybercrime, data protection and e-governance). Currently, cybersecurity is the most favored theme within the GFCE, followed by cyber-crime. However, members did state an **interest in initiatives on e-governance and data protection**, but indicated at the same time confusion concerning the definition and scope of these themes. This could explain why these themes have not been picked up as yet.

By including initiatives covering all the GFCE themes, the GFCE can truly claim a broad cyber capacity building scope. If in the end, the real interest in data protection and/or e-governance turns out to be fairly minimal, a discussion on the thematic areas and whether they are still relevant will be tabled for the next Annual Meeting.

In November and December 2016, the GFCE Secretariat contacted the GFCE members who expressed an interest in specific initiatives and have made an **inventory** of their interests and whether there are gaps and opportunities for new initiatives. This could also include suggestions for new strategic GFCE members. By matching supply and demand, the GFCE members could take the necessary steps for new initiatives.

The Advisory Board will provide advice and guidance to the GFCE members on possible ways of integrating an e-governance and/or data protection component into existing or new initiatives. This study will be shared by February for further discussion at the next Annual Meeting.

4. Timeline for 2017

As the GFCE strives towards the GCCS2017 as a momentum to present the global cyber capacity building agenda and good practices, it has to be realized that the timeline is quite ambitious. The GFCE will therefore also rely on member's active engagement.

Up to the GFCE Annual Meeting in May 2017, new initiatives will be developed to fill the gaps and the existing initiatives will focus on delivering results.

In **March/April 2017**, a **GCCS preparatory workshop** will be organized.

- The initiative leads, interested GFCE members, the Advisory Board and if required, external stakeholders, will discuss the good practices in an interactive workshop session.
- The workshop is followed by a one day session with the members whose delegates will take part in the GCCS high level discussion. The envisaged outcome of this session is a first concept of the global cyber capacity building agenda.
- To start the discussion, the analysis of all the research outcomes combined will be presented at the beginning of the session.

In **May 2017, the GFCE Annual Meeting** will take place. The aim of this meeting is to

- Discuss the first draft of the global agenda.
- Discuss the exploratory list of good practices.
- Present and discuss the preliminary outcomes of the research by the concerned parties which will feed the concept global agenda for the GCCS2017.

Discussion will take place in plenary form and continued in smaller break out groups. While the focus of the first year was geared towards presenting the individual results of the initiatives, the focus of the Annual Meeting of 2017 will be on the linkages between the initiatives and translating the outcomes to the level of good practices.

If required, a **(virtual) meeting will be organized in September/October**, to further the discussions on the good practices and the discussion on the global agenda in the months up to the GCCS.

In the margin of the GCCS, **a GFCE cyber capacity building pre-meeting** for the members and the Advisory Board will be organized to connect the last dots and finalize the list of good practices and the global capacity building agenda. This could be followed by a first discussion on the follow up on the results of the GCCS2017.

At the GCCS, the GFCE strives for the global agenda and good practices of cyber capacity building to be presented. Herewith, the GFCE members in collaboration with the Advisory Board will steer the development of GFCE wide agreed-upon and voluntary recommended good practices on cyber capacities. The recommended good practices and the global cyber capacity building agenda could form the basis for a coordinated response to cyber challenges.

As set out in the Framework Document and the Hague Declaration, the GFCE aims to organize high level meetings en margins of the future GCCS's. This does not mean that the GFCE and its future deliverables will be limited or bound to the GCCS process. The GFCE will continue looking for appropriate fora, to uphold the moment and setting the stage for similar discussions as the one foreseen for the GCCS2017.

The way forward after successful completion of the roadmap will be defining a long term strategy for the GFCE for which the "global cyber capacity building agenda" and "global good practices" can form the basis.