GFCE Workshop on Global Good Practices
&
GFCE Workshop on the Global Agenda on CCB

September 25th & 26th, 2017, The Hague

Summary by the GFCE Secretariat

Foreword

In less than two months, the Global Conference on CyberSpace (GCCS2017) in India will take place, where the GFCE community aims to present the Global Good Practices (GGP) and the Global Agenda on Cyber Capacity Building (GACCB). The GCCS2017 provides 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.

On September 25th-26th, the GFCE Secretariat organized workshops on the Global Good Practices and the Global Agenda on Cyber Capacity Building in The Hague. The workshops were organized to primarily discuss the first drafts on both the GGP and the GACCB. Representatives of the United States, United Kingdom, European Union, Microsoft, Global Cyber Security Capacity Centre (GCSCC), the Netherlands, France, Israel, Hungary, Romania, Council of Europe, FIRST, the Meridian, and IAP attended the workshop in person. Furthermore, multiple GFCE members remotely participated during the workshop on GACCB.

GFCE Workshop on Global Good Practices - September 25th, 2017

Highlights of the workshop

- The final version of the GGP document will be developed in the upcoming months towards the GCCS2017. All GFCE members are asked to fill in the questionnaire and forward this to the Secretariat.
- It is important to contemplate on how the GGP document should be communicated. Different target groups should be considered. Where high-level and operational government are interested in more policy-oriented documents, the corporate sector and technical community are likely to appreciate a more concrete and actionable document.
- When delivering a pitch on a GFCE initiative, it is important to keep your audience in mind.
- The next GGP draft is due by the beginning of October.
- The GGP and GACCB documents need to align; this will be kept in mind during the process of developing the next GGP draft.
- The GFCE Secretariat will stay as transparent and clear as possible about the process of both GGP and the GACCB.

Opening

In a joint effort the GFCE Secretariat and DiploFoundation organized a workshop on Global Good Practices (GGP). The workshop was led by Vladimir Radunoviç from DiploFoundation. The GGP, referring to particular good ways to do a practice, are comprised out of a broad range of initiatives within the GFCE community. With the input provided by the GFCE community in the past months, a first draft on GGP has been presented. This workshop provided an excellent momentum for the GFCE community to further reflect on the content of the GGP document and discuss how to move forward in communicating the GGP.

Communicating GGP's

The Diplo Foundation thanked all GFCE members for their contribution in the process of developing the first GGP draft and encouraged to send their additional feedback in the following month. The next step is to think of effective manners to communicate the GGP document. During the workshop all participants were asked to visualize a detailed profile of a community the GFCE would like to target. This effort will help in developing an effective communication strategy for the GGP document. In this regard the workshop participants presented four profile sketches for the following target groups: GCCS community; Corporate sector; Technical community; and Governmental (operational level) community.

GCCS community

The GCCS will typically be visited by high-level ministers from various countries. Visiting a conference like the GCCS suggests this target group is interested in learning about the cyber threat landscape, from both a national and international perspective. This target group will have no time to read long documents and will receive policy brief papers from their staff instead. Thus, the GGP document should be communicated via policymakers. In the GGP document the benefits for the minister and the respective nation should be clearly stated, for one it should be underlined that there is international support and collaboration. This target group is most likely to be on board if the GGPs are linked to domestic priorities and if there is opportunity to gain recognition for their country.

Corporate sector
It is suggested that parties in the private sector are often dealing with cyber security incidents and are therefore interested in learning about the GGP document. In addition, financial motives play a significant role. This target group would want the GGP document to provide complete and concrete steps on how best to deal with cyber threats. The GGP document could either be provided to a private stakeholder from its own network or be found after actively searching for a guiding document.

Technical Community
The technical community will be most interested in a GGP document that provides practical guidance. To be considered a valuable document, the technological aspect of the document needs to be on point and open for improvement. The target group could be triggered if the GGP document is framed as a way of technical innovation. There are many ways the GGP document could reach the technical community, from within their own networks or own research.

Government (operational level)
As mentioned before, the GGP document will in most cases be passed by the ministerial staff to reach high-level ministers. Hence, this target group is very important for the GFCE. Due to time constraints, it is still essential the GGP document requires little time to read. Same as the high-level minister, the ministerial staff will be interested in the GGP document if it can be linked to top ministerial priorities. Furthermore, the GGP document becomes more valuable if it includes lists of contact details and available resources that can be used to build cyber capacity. In general, many different departments in government are involved in cyber security. To have maximal impact, the GGP document should be shared interdepartmental.

DiploFoundation has recorded all presentations and will use the input of all participants to further develop a communication strategy for the GGP document.

GGP Pitches

In the second part of the workshop on GGP, participants had to give a one minute pitch of their GFCE GGP. The audience evaluated the concise pitch and offered advice on how to improve. When giving feedback, participants were asked to consider the perspective of their assigned target groups (GCCS community, corporate sector, technical community and government). The following initiatives were pitched: Cybergreen; CIIP; Awareness month; CCM; Internet Infrastructure; Glacy+; CVD; and CSIRT. The following general remarks can be made concerning the pitches:

- The participants expressed their concerns from their respective communities, this was a valuable exercise in polishing the pitches. The given feedback will be considered in perfecting the existing pitches.
- The presentation of the initiatives should be tailored to the perceived audience. The corporate community will be more interested in the concrete steps of an initiative opposed to a high-level minister that will want to hear about the strategic benefits for its country.
- When preparing to present initiatives for the GCSS, pitches should connect with a high-level audience.

Wrap-up: Next steps

DiploFoundation appreciated all remarks and will take these into consideration when developing the next GGP draft. The next GGP draft is scheduled to come out around the first half of October. Further, an important note is that the GGP document needs to have a strong link with the GACCB. The GFCE Secretariat will stay as transparent and clear as possible about the process of both GGP and the GACCB.

GFCE Workshop on Global Agenda on CCB - September 26th, 2017

Highlights of the workshop:

- Feedback on the first draft of the GACCB can be submitted till mid-October.
- All GFCE members are invited for the pre-GCCS meeting in India on the 21st of November.
- The language in the GACCB needs to be taken to the next level. Due to the audience at the GCCS2017, the GACCB should speak to the policy level to gain attention of a high-level community.
- The importance of public-private partnership, prioritizing resources and regional ownership are lacking in the current set of principles.
- It is considered to use a tag system in the GACCB to connect initiatives and the GGP's.
- Finding the right balance in developing a global agenda that is both practical and strategic is very challenging. All GFCE members are asked to help think of ways to accomplish this.

Opening

The workshop on the Global Agenda on Cyber Capacity Building (GACCB) was led by David van Duren, head of the Secretariat, and Tjarda Krabbedam, TNO. With the GACCB the GFCE attempts to develop a valuable, sustainable and global agenda on cyber capacity building and hopes therewith to strengthen cyber capacities globally. The workshop opened with a quick overview of the GACCB process provided by TNO. Furthermore, as co-chair and organizer of the GCCS 2017, India informed the GFCE community on the GCCS2017 during each remote regional call.

Next, the feedback on the first draft of the GACCB was discussed. The workshop was divided in two blocks. First, the principles and topics (chapter 2 and 3) were under review. The second block focused on the chapter on ambitions and actions (chapter 4). In addition to the representatives of the GFCE community physically present, other GFCE members participated remotely in regional calls set up during the workshop. During the regional calls, remote participants were allowed to reflect on the entire document.

Process GACCB

As a bottom-up platform, the GACCB is the result of a GFCE community effort. In the past months, TNO has collected input from the GFCE community through workshops, interviews, multistakeholder conference calls and questionnaires. The next draft GACCB document is planned for mid-October. After presenting the second draft, there will be some further consultation with the GCCS community in October – November. Finally, the GACCB will be presented during the GCCS2017 in New Delhi on 23-24 November.

Information on GCCS 2017

Mr. Dhawal Gupta of the Ministry of Electronics and Information of India remotely participated in all regional calls to inform the GFCE community about the GCCS. The main theme of the conference is "Cyber4All: A Safe, Secure and Inclusive Cyberspace for Sustainable Development" which is comprised out of four subthemes. The subthemes are Cyber4Growth; Cyber4DigitalInclusion; Cyber4Security; Cyber4Diplomacy. The GFCE will have the opportunity to present the GACCB during a plenary session of fifteen minutes on November 24th. Further all GFCE members are invited for the GFCE pre-GCSS meeting on November 21st.

Discussion on Cyber Capacity Building Principles and Topics

First the audience reflected on chapter 1 – 3 of the GACCB. This included the introduction, the Cyber Capacity Building principles which are based on the Busan Partnership for Effective Development Co-operation and the cyber capacity building topics. The following comments were made:

- **Shared language:** It is important to establish a common language among the GFCE community and beyond. The notion of shared language could be constructed in either the introduction or principles section of the GACCB. Further language should be consistent in both the GACCB and GGP document.
- **Areas of CCB:** While most initiatives are on cybersecurity, cyber capacity building does include efforts in areas such as cybercrime and e-governance. There should be a clear understanding of what CCB refers to.
- **Principle of Transparency**: The principle of transparency is ambiguous and should be further explained.
- **Principle on prioritization of resources:** the necessity to prioritize resources should be added. As multiple participants mentioned, not all members will have the resources to address all cyber capacity building areas at once.
- **Importance of PPP and social engagement:** It should be emphasized that the GFCE is a multi-stakeholder platform and consults with a broad range of parties (not only government). It is suggested to add some notes to the principle on ‘partnership’.
- **Importance of regional CCB:** The principles should encompass the importance of regional cyber capacity building. It was agreed that CCB should first respond to issues on a regional level, and from there lay the basis for national and global action.
- **Introduction CCB topics:** In chapter 3, adding a short opening for each topic is proposed. This could either be about concrete actions or policy aims, depending on the target group. In the case of a high-level meeting like the GCCS2017, it is preferred to stay within the policy framework. Concrete actions could perhaps be added in annex.

Discussion on Ambitions and Actions

The main focus of the second part of the workshop was the Ambitions and Actions (chapter 4) in the GACCB document, which part is still work-in-progress. The GFCE members were asked to specifically provide feedback on the third column ‘actions’, which was left open in the first draft. The term ‘actions’ refers to what members could contribute to the GFCE ambitions in CCB. Actions can range from funding to setting up a new initiative. The following remarks were made:

- **Actions:** There was some critic on using the term ‘actions’ in the GACCB document. Participants agreed that the term is not well chosen and they proposed to change this to ‘recommendations’. The term ‘action’ is perceived as giving the GFCE too much accountability in the process of CCB and gives the illusion of there being only one way to achieve the stated ambitions. The term ‘recommendations’ clarifies that this last part of the GACCB is merely setting an example for future CCB efforts.
- **Concrete examples of CCB:** It is deemed important to include some concrete examples of CCB by the GFCE community in the GACCB. One way this could be done, is to create a stronger link between the GGP document and the GACCB.
- **Balance between practical and strategic agenda:** The challenge is to maintain a balance between a practical and strategic agenda. It is important to be readable for policymakers but at the same time stay actionable. The GACCB will be presented at the GCCS in India, and thus it should be tailored to gain attention of a high-level community. Participants agree that the

GACCB for now should stay on a more strategic level. After the GCCS, more action oriented language and steps are desired. To keep private stakeholders on board, adopting an actionable approach is essential.

Regional calls

Throughout the workshop, three regional calls were scheduled. Representatives from Australia, Japan, Symantec, ECOWAS, Senegal, CTO, OAS and the World Bank remotely participated. Please find the most important remarks below:

- **Positive feedback**: Overall the GACCB received positive feedback and was recognized as being a valuable document.
- **Future CCB efforts Australia:** Australia noted that the topics in the GACCB aligned with their current and future efforts in cyber capacity building. Possibly, Australia will introduce new GFCE initiatives in the Pacific Islands.
- **Cross-cutting CCB topics:** It is noted that many cyber capacity building topics can be seen as cross-cutting and that these should not be exclusive. It was suggested to organize the document in a way that multiple topics can be tagged in one initiative. This could simultaneously create a stronger link between the GGPs and GACCB. Further the links between the topics can perhaps be visualized in the lotus flower.
- **Current initiatives on CCB:** The option of adding an annex of all current initiatives on cyber capacity building in both the GFCE community and beyond is discussed. While this could make the GACCB more inclusive and identify the gaps in cyber capacity building, it is decided to include only GFCE initiatives. It is emphasized that the GACCB will be presented during the GCCS for a high-level meeting, meaning that the initiatives are only illustrative to inspire other stakeholders.
- **Future CCB initiatives of Symantec:** Symantec has an interest in projects in IoT security regulation, reporting on cyber threat landscape in Asia and making a guide on how to have a successful public-private partnership. These projects connect with the topics identified in the GACCB.
- **GFCE members at GCSS:** It would be good to have many GFCE members attend the GCCS. Next to funding, it is important to ensure the right employees are send to the conference. It is important that the work on cyber capacity building is continued back home.
- **Cross cutting themes CCB:** It is emphasized that both funding and international cooperation are cross-cutting for all CCB efforts.
- **Presentation GACCB during GCSS:** The impact of the GACCB will depend greatly on the presentation during the GCCS. Presenting a global agenda, which has a low threshold of commitment, is a good way to approach the GCCS community. The GFCE members agree that signing a declaration on CCB would be too formal.
- **Ambitions GACCB:** The GACCB should aim to focus on what needs to be done in the future rather than map what has already been undertaken. While it is harder to formulate shared future ambitions that all GFCE members accept, this will have a much bigger impact on the global community.
- **Existing CCB efforts of GFCE:** However, the GFCE should find a way to incorporate the existing initiatives in the GACCB as well. It is discussed that a complete overview of all existing CCB efforts would be very valuable. The Oxford portal is working to map all global CCB, but is not (yet) able to provide a complete overview. As the list on CCB is ever growing, a long-term solution could be to set-up a portal in which stakeholders are responsible for uploading their own project lists.

Wrap-up & end of session

The workshop participants were asked to share their takeaways from the workshop with the group. All agreed that it is necessary to find the balance between a high-level policy oriented and an action oriented approach. The GACCB defines the GFCE priorities in CCB, a document that all relevant stakeholders can rally behind and apply to their own unique circumstances. Its value is that it makes a stronger point – not as a single stakeholder but because it is the result of a global effort. The workshop showed that there are many different perspectives on how the GACCB could take form. First and foremost, the GACCB should be a clear example of the GFCE taking leadership in global cyber capacity building.

TNO thanks the GFCE members for their valuable input, which will now be used to further develop the GACCB. While much progress is made, there is still much work to do. In about two weeks, the second draft on GACCB will be presented to the GFCE community. The biggest challenge will be to create an agenda that will resonate with the GCCS community and at the same time echoes the action-oriented approach of the GFCE.