To: Ambassador Jürg Lauber, Chair of the Open-ended Working Group
13 November 2020

Excellency,

On behalf of the Board of Directors of the Global Forum on Cyber Expertise ("GFCE") Foundation, we submit the following comments on the discussion questions for the third round of informal meetings of the Open-ended Working Group (OEWG) on developments in the field of information and telecommunications in the context of international security. We commend your efforts in finding innovative ways to continue the work of the OEWG in these exceptional circumstances and once again, bringing awareness and emphasis to the importance of capacity building.

The GFCE Foundation Board has previously submitted comments on the initial pre-draft which we refer to in our comments below and attach as still operative (see Annex, page 4 – 6). As the mission of the GFCE is to facilitate coordination of global cyber capacity building, we have once again limited our comments to the capacity building section of the discussion.

5.1 What platforms could be used to facilitate coordination and resourcing of capacity building and how can such a platform coordinate with other relevant entities within and outside the UN?

First, we appreciate the suggested willingness to cooperate with platforms outside the UN. We would like to reiterate and put forth the GFCE as the platform for the coordination and resourcing of capacity building. Since it was established in 2015, the GFCE has acted as the worldwide coordinating and facilitating body for Cyber Capacity Building (CCB), with the objective to strengthen cyber capacity and expertise globally. From 42 members in 2015, the GFCE multi-stakeholder network has grown to 86 members and 37 partners including over 55 UN Member States as well as UN entities such as ITU, UNODC and UNIDIR, and regional organizations (e.g. AUC, OAS, EU, OSCE, etc.). As a neutral, apolitical and community-driven platform, we strengthen international cooperation by matching needs, resources and expertise while making practical knowledge and proven solutions available to the global community through a dedicated CCB knowledge portal (www.CybilPortal.org). In addition, the GFCE has organized over 50 regional and global events on CCB with outstanding programs, speakers and workshops. By now, the GFCE has established on the ground presence in the Pacific, Africa, Europe, Asia, and the Americas, with the GFCE Community representing all continents, and we will continue to emphasize regional efforts to work closely with regional platforms while maintaining a global reach.

We wholeheartedly agree that global coordination needs to be strengthened, that is our founding principle and mission, but avoiding duplication and highlighting existing efforts is important to ensuring scarce resources are used effectively. In practice, a newly formed UN coordination mechanism would likely be duplicative of existing efforts, including the GFCE. It would also be resource intensive and, more importantly, would likely face substantial challenges in being effective. Among other things, it would be difficult for the UN to facilitate or coordinate NGO, private sector or other non-state capacity building activities – something that the revised pre-draft acknowledges as important and that is already a cornerstone of GFCE activities.

Global coordination is important to amplify capacity building efforts and ensure greater effectiveness and efficiency. The GFCE's efforts to build regional nodes and increase its regional focus is an efficient approach to realizing global coordination, as this highlights regional perspectives and priorities for capacity building. Furthermore, the GFCE has the vision to cooperate and connect with other existing platforms in this field, including the UN, to achieve its mission to strengthen cyber capacity building and expertise globally.

Amongst these platforms, we would like to highlight that the GFCE is in a unique position as it is already playing a key role in facilitating and coordinating efforts because of its neutrality, multi-stakeholder community, and bottom-up approach, which bridges the gap between policy and practice. Furthermore, with the development of the GFCE Global Cyber Capacity Building Research Agenda, the GFCE hopes to take a major step forward to lead the addressing knowledge gaps and obstacles cyber capacity building. Acknowledging that the UN has a key role in raising awareness for cyber capacity building, and in particular in the implementation of norms and confidence building measures, the GFCE hopes to work closely together with the UN to explore how the GFCE can further support the outcomes of the international cyber stability negotiations, especially as they relate to cyber capacity building.

To increase resourcing of capacity building, the GFCE recognizes that it is necessary to secure high-level, political recognition of the importance of capacity building. As mentioned in our comments on the pre-draft, it would be useful for the UN to address a longstanding issue with cyber capacity building: that it is largely not integrated into the larger development community agenda or the UN Sustainable Development Goals. By integrating cyber capacity building and funding as a foundational pillar for national development at large, that alone could have a tremendous impact on the ability to conceive and execute vital cybersecurity programs, and importantly, ensures that citizens can trust and have confidence in the digital tools offered. Moreover, by integrating cyber capacity building into UN development agendas, cyber capacity building efforts could potentially increase globally and become a concreate measure of cyber norms adoption.

The GFCE also has plans to convene a high-level political conference in 2021 in collaboration with states, development organizations and others, to raise the profile and allocation of resources for Cyber Capacity Building and encourage global coordination and cooperation between existing entities. For the reasons listed above, we hope that the UN will recognize the GFCE's commitment to work together to support the facilitation and coordination of cyber capacity building globally.

5.2 Do the categories of Partnerships, People and Process in paragraph 57 of the revised pre-draft capture the breadth of principles articulated by OEWG delegations?

The GFCE's principles for cyber capacity building, submitted as input to the pre-draft, are contained in the GFCE Delhi Communiqué on a Global Agenda for Cyber Capacity Building. These principles are a result of a year-long process of conducting extensive consultations and research, which were unanimously endorsed by the GFCE Community at the Global Conference of Cyber Space in Delhi late 2017.

We were pleased to see that the principles listed under Partnerships, People and Process share some similarities with the Delhi Communiqué principles related to capacity building. Specifically included are those that relate to national ownership, shared international commitments such as in human rights, inclusivity, information sharing and others. We would like to further suggest the following additions to the current principles, which are drawn directly from the Delhi Communiqué:

- the need for multi-stakeholder participation;
- the necessity for fostering local expertise by using and creating regional expert hubs;
- the value of international cooperation; and
- shared principles for cooperation such as trust, transparency and accountability.

What is notably absent from the principles but would be important to include is the encouragement of all relevant stakeholders to allocate funding and expertise for capacity building. It would be

extremely helpful for the UN to make clear in its principles that capacity building is a major priority and a pre-condition to achieve peace and stability in cyberspace, and that an increase in the pool of funding for capacity building is necessary to significantly expand the resources available for cyber capacity building globally.

We hope that these comments will be helpful to you and we stand ready to assist and support you in any way that we can. For more information on the GFCE, please contact the GFCE Secretariat.

Sincerely,

Chris Painter

President of the GFCE Foundation

ANNEX: GFCE Foundation Board Comments on OEWG Initial Pre-Draft Report

To: Ambassador Jürg Lauber, Chair of the Open-ended Working Group
15 April 2020

Excellency,

On behalf of the Board of Directors of the Global Forum on Cyber Expertise ("GFCE") Foundation, we submit the following comments on the initial pre-draft of the report of the Open-ended Working Group on developments in the field of information and telecommunications in the context of international security.[1] As the mission of the GFCE is to facilitate coordination of global cyber capacity building, we have limited our comments to the capacity building sections of the pre-draft. As you are aware, the GFCE is a multi-stakeholder community of more than 115 members and partners consisting of governments, IGOs, private entities, academia and implementers from all regions of the world; sharing the vision to fully reap the benefits of ICT through a free, open, peaceful and secure digital world. GFCE members and partners include UN entities, such as the ITU and UNODC, and regional organizations such as the OAS, African Union and EU. The GFCE's mission is to act as a worldwide coordinating body for Cyber Capacity Building (CCB). It strengthens international cooperation by matching needs, resources and expertise. The GFCE makes practical knowledge and proven solutions available to the global community through a dedicated CCB knowledge portal (www.CybilPortal.org). In addition, it organizes regional and global events on CCB with outstanding programs, speakers and workshops. Recently the GFCE Foundation was launched in order to help grow and mature the GFCE, as well as provide long term sustainability and independence.

First, we welcome the pre-draft's focus on cyber capacity building as a major foundational pillar of international security and stability in cyberspace. We support much of the current language that notes why capacity building is important, how it helps empower "all States and other relevant actors to fully participate in the global normative framework, while also contributing to shared commitments such as the 2030 Sustainable Development Agenda," how it helps states deal with transnational cyber threats and the need for capacity building across a spectrum including technical, diplomatic and policy disciplines. We also strongly support language that a multi-stakeholder approach to capacity building is vital as well as language affirming that gender inequality should be addressed.

While much of the pre-draft language is strong, we believe that some of the discussion and subsequent recommendations do not fully capture both state and nonstate interventions on capacity building made during OEWG sessions nor provide an effective, workable solution. First, in the discussion, while the pre-draft notes that: "States stressed that there was a need for greater coordination in capacity-building efforts," it fails to note that many states made the point that there should not be a duplication of efforts and many said that the GFCE was in fact performing this coordination and facilitation role. Of course, we agree that global coordination should be strengthened, that is our founding principle and mission, but avoiding duplication and highlighting existing efforts is important to ensuring scarce resources are used effectively.

Acknowledging that the UN has an important role in cyber capacity building, and the GFCE wants to work closely with the UN and UN institutions on this vital issue, one of the pre-draft

[1] These comments are submitted by the GFCE Foundation Board and reflects their views. They may not fully reflect the views of all of the GFCE's many partners and members.

recommendations appears to suggest that the UN create a new mechanism which we believe would be duplicative and of limited effectiveness.

The pre-draft recommendation is:

> *"The Secretary-General be requested to establish a global mechanism for enhancing coherence in capacity-building efforts in the use of ICTs, possibly in the form of a facilitation mechanism, in coordination with existing efforts, including at the regional and sub-regional levels. States in a position to contribute expertise or resources to the development of such a mechanism are encouraged to do so."* (para. 68d)

In practice, a newly formed UN coordination mechanism would likely be duplicative of existing efforts, including the GFCE. It would also be resource intensive and, more importantly, would likely face substantial challenges in being effective. Among other things, it would be difficult for the UN to facilitate or coordinate NGO, private sector or other non-state capacity building activities – something that the current pre-draft acknowledges as important and that is already a cornerstone of GFCE activities.

That is not to say that the UN does not or should not play an important role in cyber capacity building – it does and it should. For example, the existing pre-draft's call for capacity building principles can be helpful when endorsed at a UN level. The GFCE's principles, submitted as input to the pre-draft, are contained in the GFCE Delhi Communiqué on a Global Agenda for Cyber Capacity Building.[2]

---

[2] The language of the GFCE Delhi Communiqué relevant to capacity building principles is:

- "10. Recognizing the importance of cross-cutting capacity issues, we encourage countries to conduct cyber capacity building in ways that take account of:
  a. The need for participation by all stakeholders in strengthening cyber capacity building;
  b. The need for treating the protection of critical information infrastructure and cyberspace as a shared responsibility that can best be accomplished through collaboration among all relevant stakeholders
  c. The value of international cooperation;
  d. The necessity for fostering local expertise by using and creating regional expert hubs as capacity building multipliers;
  e. The importance of information sharing by all stakeholders;
  f. The benefits of cyber security research and innovation;
  g. The multidisciplinary nature of cybersecurity, and the diversity of skills and knowledge required; and
  h. Capacity building's support to international security, including the applicability of international law, agreed voluntary norms and confidence building measures.
- 11. In support of stronger capacity building co-operation we endorse the following shared principles (inspired by the Global Partnership for Effective Development Cooperation, and applied to cyber capacity building) – consistent with our agreed international commitments on human rights, decent work, gender equality, environmental sustainability and disability – for cyber capacity building:
  i. Ownership: nations need to take ownership of capacity building priorities focus on sustainable developments;
  ii. Sustainability: obtaining sustainable positive impact should be the driving force for cyber capacity building;
  iii. Inclusive partnerships and shared responsibility: effective cyber capacity building requires cooperation among nations, through a multi-stakeholder approach; and
  iv. Trust, transparency and accountability: transparency and accountability play a key role in establishing trust, which is necessary for effective cooperation.
- 12. We encourage all relevant stakeholders to allocate funding and expertise for capacity building, applying the above principles and coordinating their support with other capacity building initiatives."

It would also be helpful for the Secretary-General to make clear that capacity building is a major priority and that existing coordination mechanisms and capacity building efforts should be supported and prioritized by all member states. Another possible positive message would be for the Secretary-General to call for states to increase funding for capacity building. For even greater impact, the Secretary-General could address a longstanding issue with cybersecurity capacity building: that it is largely not integrated into the larger development community agenda or the UN Sustainable Development Goals. As you are aware, traditional development organizations have largely excluded or not given priority to cybersecurity programs. If the Secretary-General called on these organizations to integrate cybersecurity capacity building and funding as a foundational pillar for capacity building at large, that alone could have a tremendous impact on the ability to conceive and execute vital cybersecurity programs. Linking cybersecurity capacity building as a foundational element for many of the Sustainable Development Goals would similarly send a powerful message.

In furtherance of this, the Secretary-General could be requested to help convene a high level meeting with organizations like the GFCE (potentially including some implementers and some of the new cyber-focused organizations), states, development organizations and others to raise the profile and allocation of resources for Cyber Capacity Building and encourage global coordination and cooperation between existing entities. We believe that this could be far more effective than trying to establish a new and potentially duplicative UN coordination structure.

Again, we applaud your efforts in both organizing the OEWG and producing an initial pre-draft report that emphasizes the importance of capacity building. We hope that these comments will be helpful to you and we stand by to assist you in this important task in any way we can.

Sincerely,

Chris Painter

President of the GFCE Foundation