Contribution to the Second Substantive Session of the Open-Ended Working Group on the security of and in the use of information and communications technologies 2021-2025 (OEWG)

Contribution of the Global Forum on Cyber Expertise (GFCE)
Thursday 31 March 2022

On behalf of the Board of the Global Forum on Cyber Expertise (GFCE) Foundation, we submit the following contribution for the second substantive session of the Open-ended Working Group (OEWG) on developments in the field of information and telecommunications in the context of international security 2021-2025. The GFCE is a multistakeholder community of over 150 members and partners including member states, international and regional organizations, the private sector, civil society and academia dedicated to the global coordination and promotion of cyber capacity building.

In this contribution, we make recommendations on the possible role of the OEWG and the United Nations vis-à-vis capacity building, highlight the importance of a multi-stakeholder approach, and put forth the GFCE as a mechanism for facilitating the implementation of capacity building measures. Further recommendations and substantiation of this position can be found in the reading section at the end of this submission.

Many countries still lack the technical, institutional and policy capability to respond to malicious cyber events, including the capability to cooperate internationally, and many lack the ability or expertise to fully participate in the many international debates that are shaping the future of cyberspace. A substantial answer to both preparing countries to deal with cyber threats and ensuring they can more fully participate in policy implementation is cyber capacity building. Yet, cyber capacity building remains underprioritized and underfunded—particularly when compared to other areas of traditional development, such as physical infrastructure, water, and health that are themselves increasingly dependent on digital systems and vulnerable to cyberattack.

Placing greater emphasis on cyber capacity building in high-profile multilateral discussions at the UN (GGE, OEWG and AHC) has immense potential to elevate the profile and prioritization of cyber capacity building. This can lead to greater dedication and commitment by countries and other non-State actors to identify and address needs of developing countries. In defining a role for the UN and more specifically the OEWG vis-à-vis implementation of capacity building measures, we urge the UN to first consider leveraging existing platforms and initiatives to avoid duplication of such efforts and inefficient use of scarce resources. The second thing to consider is where the UN can be most effective and demonstrate biggest impact.

Recommendation 1: Prioritize leveraging existing initiatives over establishing a new structure

The Chair's suggested questions in the workplan to guide the discussions on capacity building focus, in part, on the on possible institutional roles of the UN and OEWG. One question appears to suggest an operational coordination role for the UN through the appointment of a new capacity building contact point (though the role of that contact point is not further elaborated). Whilst it goes without saying that the UN should certainly coordinate its own activities and find efficient

ways to work with existing outside efforts, creating a new external coordination structure would likely be duplicative of existing efforts, including the GFCE. Depending on its structure and role, such a mechanism would also be resource intensive and, more importantly, would likely face substantial challenges in being effective since it would be difficult for the UN to facilitate or coordinate non-state (such as civil society, private sector, etc.) capacity building activities. While we wholeheartedly agree that global coordination needs to be strengthened, and that the UN has an important role in capacity building, the UN should avoid reinventing the wheel and instead look to bolster existing coordination platforms by lending support and working with those initiatives.

Given the GFCE's existing coordination function on capacity building and its established network, the UN could leverage our global platform to facilitate and coordinate assistance requests. A concrete measure could therefore be to officially recognize existing capacity building platforms and initiatives to promote complementarity and form official partnerships with such initiatives including the GFCE.

Recommendation 2: Encourage greater information-sharing on capacity building activities.

The UN could encourage States and other actors to share information on their capacity building projects and activities, which would serve to increase transparency and enable better coordination. Though some States and organizations share some information on their projects and activities, the vast majority of funders, implementers or beneficiaries are still reluctant to share details on ongoing projects. A lack of sharing deprives other players and regions from benefiting from lessons learned, it hampers coordination, leads to potential duplication, and limits helpful input that the sharing party might otherwise receive. Whilst some have legitimate concerns regarding confidentiality of proprietary information, transparency and the greater sharing of information regarding capacity building should be encouraged as the default practice.

In addition to details on specific projects, it would also be beneficial for actors to share information on outcomes, best practices, and the effectiveness of activities when a project has concluded. The GFCE supports suggestions for States to share information regarding the challenges they have faced with regards establishing and implementing capacity building efforts alongside the successes. Divergences in information regarding levels of implementation, particularly at the regional level, can have a negative effect on the ability and expectations of stakeholders to with regards capacity development. Better understanding of existing policy and practical activities of States and organizations alike is therefore essential.

In this regard, the GFCE supports the launch of the National Survey of Implementation of the United Nations recommendations on the responsible use of ICT's by States in the context of international security as a means of encouraging States to assess their own priorities, needs and resources, thereby advancing cyber capacity building. The GFCE has a longstanding history of contributing to the Cyber Policy Portal and continues to leverage its membership towards the goal of enriching the information available on this platform. For example, through its Working Groups, GFCE Members provide updates on policy and strategy developments which are then shared with UNIDIR.

Similarly, through regional programs the GFCE has been conducting foundational mapping exercises which can also complement the aims of the Survey. The latest mapping efforts leverage the GFCE's strong partnerships with regional organizations such as the Organization of American States (OAS), Organization of Security and Cooperation in Europe (OSCE) and ASEAN alongside their respective Member States, with improved regional coordination and information sharing one of the key benefits and objectives of the partnership with OAS as the GFCE Hub in the Americas.

As a corollary to the Survey, the UN could also reference the GFCE's Cybil Portal – a unique knowledge hub for cyber capacity building and the only source of project information to encompass the full range of international cyber capacity building projects. The Cybil Portal is fast becoming a comprehensive source of basic project information, with information on over 800 projects and 750 resources in its repository and is a good starting point for setting a baseline for mapping activities globally.

The Cybil Portal includes information on capacity building projects and resources of non-governmental actors as well as States. Considering that the Survey will include information on States' capacity building efforts, in addition to information on the implementation of agreements on international law, norms and CBMs, it will be important to continue to coordinate the development of these portals in a way that they can be complementary and not duplicative of each other.

With regard to existing and planned capacity building activities, States could commit to providing key information on those projects at regular intervals and making that information public on the Cybil Portal in a transparent way. Such information can support others in developing similar activities and allow for more effective recording of what activities are being conducted.

Recommendation 3: Establish clearer links between cyber capacity building and development, and increase resources for actionable commitments

The development community and the cybersecurity community share related goals of strengthening digital capacity building, including the ability to effectively use advanced technologies while simultaneously ensuring that citizens remain safe, protected, and productive online. Despite these similar aims, the two communities operate primarily within their own disciplines, rarely partner, and embed cybersecurity activities within digital development projects.

The relative lack of attention and resources for cybersecurity capacity building is attributable to its lack of integration with larger development programs or digital strategies. For example, the UN Sustainable Development Goals (SDGs) have attracted both political attention and substantial resources. While cybersecurity is a key enabler of many of those goals, there is no formal clear acknowledgement of that relationship.

In addition, the donor community's reliance on metrics to steer investment means that the cybersecurity capacity building community will need to create an empirically convincing argument that an absence of better cybersecurity leads to demonstrably worse outcomes. If the need to integrate cybersecurity into development is empirically convincing, the cybersecurity community

more broadly has yet to develop truly useful measurements to evaluate cybersecurity and cybersecurity capacity building interventions.

Lacking these metrics, it becomes difficult to craft meaningful, empirically driven arguments for what capacity development interventions produce the most positive outcomes. Better outcome-oriented metrics are needed to identify and communicate these good practices, whether government policy interventions, corporate policies, or technological interventions

The UN could address this by stating for example that cyber capacity building can be instrumental in achieving the SDGs. Through the auspices of the UN framework, States should encourage more data-driven guidance for cybersecurity good practices, cybersecurity community awareness of and participation in key dialogues in the development community around the use of metrics and identification of good practices in capacity development.

In addition, the OEWG could also build on work of the previous OEWG and GGE statements that countries should further support and resource capacity building, translating those commitments into action. Many states are currently investing in cyber capacity building on a project basis, and those efforts should be built upon and used to catalyze other donors and implementers. Measures aimed at increasing the pool of resources for cyber capacity building should ensure the continuity and sustainability of a project (for example continuity of the program, staff, equipment, etc.) by programming funds into the country's national budget.

Recommendation 4: Ensure an inclusive process for multi-stakeholder actors to contribute, especially on capacity building

While acknowledging that decision making within the context of the UN and OEWG is a multi-lateral and state-led process, the OEWG should seek to ensure that non-State actors are provided avenues to share input and advice especially on capacity building. Effective cyber capacity building requires open channels for dialogue and cooperation between both state and non-state actors, and this has also been recognized in the recent OEWG and GGE reports to varying degrees. Therefore, discussions on capacity building must be premised on an inclusive, multi-stakeholder process.

The need for multi-stakeholder participation to strengthen capacity building is one of the principles of the GFCE Delhi Communiqué on a Global Agenda for Cyber Capacity Building, which has been endorsed by all GFCE Members and Partners. Some examples of areas where non-State stakeholders have been demonstrating value include but are not limited to:

- Funding and/or implementing capacity building activities;
- Supporting stakeholders through research;
- Producing knowledge products and sharing expertise;
- Bridging gaps between technical and policy communities;
- Ensuring sustainability of capacity building through local ownership;
- Measuring Cyber Capacity Building impact;
- Ensuring human rights and gender are considered in the design of projects;
- Linking capacity building to the sustainable development goals.

As a thriving multi-stakeholder platform, the work and achievements of the GFCE is a testament to the value of multi-stakeholder inclusion and collaboration, demonstrating that such a process has the major benefit of trust building between States and non-governmental actors.

Recommendation 5: Endorse the GFCE as a platform to advance and facilitate agreed upon capacity building measures

Since 2015, the GFCE has been harnessing and consolidating existing capacity building efforts through its ecosystem to strengthen coordination, facilitate knowledge sharing, and connect assistance requests with support or resources. From 42 members in 2015, the GFCE has grown its multi-stakeholder network to over 150 members and partners, including 65 UN Member States as well as UN entities such as the ITU, UNODC and UNIDIR, as well as many intergovernmental and regional bodies such as the OAS, the African Union, and the OSCE.

The GFCE has a unique position as it is already playing a key role in facilitating and coordinating capacity building efforts, made possible by its neutrality, multi-stakeholder community, and bottom-up approach. Furthermore, it has developed and maintained a flexible and diverse ecosystem that is geared towards the needs of the community and that mobilizes multistakeholder engagement by design. The ecosystem includes tools like the GFCE's Research Agenda, Cybil Portal and Clearing House mechanism, as well as structures such as the GFCE Working Groups and Regional Hubs.

To realize a demand driven approach to capacity building and to empower local capacity building communities, the GFCE's started to build regional nodes and further increase its regional focus over the last 2 years. A regional approach is also favourable because countries within a region tend to share similarities in priorities and are seen to be able to reach a common understanding, agreement or way forward more easily than in other multilateral fora. Furthermore, a regional approach can be instrumental in improving regional collaboration and knowledge sharing amongst stakeholders in the region. As capacity building requires trust between implementers and the beneficiary community to ensure sustainable and long-term impact, the GFCE is committed to connecting and collaborating with regional organizations/centres and key leaders to bolster its regional efforts. The establishment of GFCE regional hubs and liaisons in five regions will support needs analysis, regional coordination and delivery of capacity building support from the GFCE community.

To expand coordination efforts and bolster support for the Community, the GFCE recognizes that more needs to be done to increase high-level awareness and widen the pool of resources available. To this end, the GFCE is co-organizing a Global Conference on Cyber Capacity Building in November 2022, in partnership with the World Bank, World Economic Forum and Cyber Peace Institute, and with the support of several Member States. The Conference aims to secure high-level awareness for international cyber capacity building, strengthen the coordination of efforts and significantly increase allocation of resources. Among other things, the goals of the Conference are to:

- Establish a Global Coalition to coordinate efforts and resource mobilization on CCB.
- Develop an International CCB Agenda with regional chapters.
- Enhance CCB efforts by accelerating current multi-stakeholder cooperation and public-private partnerships.
- Provide routes to implementing accepted international policy recommendations on CCB in multiple sectors.
- Raise decision-makers' awareness of how cybersecurity and CCB support digital, social and economic development, in line with the Sustainable Development Goals (SDGs); and
- Build bridges between the traditional development community and the cyber security capacity building community.

Given our existing efforts and future plans, the GFCE is well-suited to help take forward and facilitate capacity building measures agreed at the OEWG. Therefore, 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.

Further reading:

1. Prioritizing Capacity Building as a Foundation for Cybersecurity and Stability – Christopher Painter (Link)

2. International Cyber Capacity Building: Global Trends and Scenarios – Robert Collett and Nayia Barmpaliou (Link)

3. Integrating Cyber Capacity into the Digital Development Agenda – Melissa Hathaway and Francesca Spidalieri (Link)