Contribution to the Third 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 by the Global Forum on Cyber Expertise (GFCE) Foundation Board

Monday 25 July 2022

On behalf of the Global Forum on Cyber Expertise (GFCE) Foundation Board, we submit the following contribution for the third 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 an apolitical multistakeholder community[1] of over 165 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 reflect on the draft annual progress report as well as the discussion questions presented in Annex C of the Chair's Written Statement dated 22 June 2022.

[1] The list of stakeholders that make up the GFCE community include:

Member States

Argentina; Australia; Austria; Bangladesh; Belgium; Benin; Botswana; Cameroon; Canada; Chile; Côte d'Ivoire; Czech Republic; Dominica; Dominican Republic; Estonia; Ethiopia; Finland; France; Gabon; Germany; Ghana; Guatemala; Hungary; India; Israel; Japan; Kenya; Kingdom of Lesotho; Latvia; Liberia; Luxembourg; Malaysia; Mauritius; Mexico; Morocco; New Zealand; Nigeria; Norway; Papua New Guinea; Peru; Philippines; Republic of Congo; Republic of Korea; Romania; Rwanda; Senegal; Serbia; Sierra Leone; Singapore; Somalia; Spain; Suriname; Sweden; Switzerland; Tanzania; Thailand; The Gambia; The Netherlands; Tunisia; Turkey; Ukraine; Vietnam.

Non-State Stakeholders

Africa Cybersecurity and Digital Rights Organisation (ACDRO); Africa Cybersecurity Resource Centre (ACRC); AfricaCERT; African Capacity Building Foundation (ACBF); African Civil Society on the Information Society (ACSIS); African Union; African Union Development Agency NEPAD (AUDA-NEPAD); AFRINIC; AFRIPOL; Alliance for Securing Democracy (ASD); APNIC; AT&T; AustCyber; Australian Strategic Policy Institute (ASPI); BAE Systems; Capgemini; Carnegie Endowment for International Peace (CEIP); Center for Cybersecurity Policy and Law; Chatham House; Cisco Systems; Commonwealth Telecommunications Organisation (CTO); Council of Europe; CREST; CYAN; Cyber Capacity Unit (CCU); CyberGreen; CyberLite; CyberPeace Institute; CyberSafe Foundation; Cybersecurity Capacity Centre for Southern Africa (C3SA); CYDIPLO; CYSIAM; DAI; Deloitte; Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ); DiploFoundation; EastWest Institute; ECCAS; Economic Community of West African States; e-Governance Academy (eGA); ESET; EU CyberNet; European Cybercrime Training and Education Group (ECTEG); European Union; Europol; FireEye; Forum of Incident Response and Security Teams (FIRST); FS-ISAC; Fundación CAPA 8; Geneva Centre for Security Sector Governance (DCAF); Get Safe Online; Global Cyber Alliance; Global Cyber Security Capacity Centre (GCSCC); Global Partners Digital; Hewlett Packard; Huawei; IBM; INCIBE; InFuture Foundation; INsig2; Insight; Institute of Cyber Security for Society (iCCS); International Association of Prosecutors (IAP); International Chamber of Commerce (ICC); International Foundation for Electoral System (IFES); International Telecommunication Union (ITU); INTERPOL; IPANDETEC; KPMG; Liberia Cyber Crime Prevention and Mitigation Agency (LCCPMA); Meridian Community; Microsoft; MITRE Corporation; NASSCOM; New America; NI-CO; NRD Cyber Security; Norwegian Institute of International Affairs (NUPI); Oceania Cyber Security Centre (OCSC); Open CSIRT Foundation (OCF); Organization for Security and Co-operation in Europe (OSCE); Organization of American States (OAS); Palo Alto Networks; Potomac Institute for Policy Studies; Protection Group International (PGI); Registry Africa Ltd; Smart Africa; Software Engineering Institute (SEI); Standard Chartered Bank; Symantec; Telstra; The Center for Cyber Security and International Relations Studies (CCSIRS); ThirdWay; TNO; Torchlight; United Kingdom; United Nations Economic Commission for Africa (UNECA) ; United Nations Institute for Disarmament Research (UNIDIR); United Nations Office on Drugs and Crime (UNODC); United States of America; Vodafone; West and Central African Research and Education Network (WACREN); World Bank; ZA Central Registry (ZACR).

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

Previous OEWG reports have been clear that capacity building is a foundational pillar in both building better technical cybersecurity for countries around the globe and achieving a more inclusive and coherent international set of international cyber policies. We welcome and support the continued emphasis on capacity building in the recent draft progress report. We also welcome recent additions concerning the relationship between cyber capacity building and the UN Sustainable Development Goals, as well as the importance of gender balance. However, there is still room to include language on strengthening existing efforts and initiatives, including those by multistakeholder actors. While there is mention of regional and subregional capacity building efforts and centers, global efforts and centres of excellence such as the GFCE are absent from the text. In light of this, there could be recognition of the substantial work, both completed and ongoing, in this space. .

The UN does and should continue to play an important role in capacity building but some of the proposed recommendations in the draft report would benefit from further exploration to define what they would look like in practice and whether they would be helpful. For example, with respect to the recommendation to designate an ICT capacity-building focal point within the UN with the responsibility to foster coordination of capacity building, further clarity would be useful regarding how this would work with and support existing capacity building coordination mechanisms within regional organizations and with global platforms such as the GFCE. It would also be valuable to outline how this position would be resourced and how it could effectively work with the variety of non-state stakeholders that often fund and implement capacity building programs. In the GFCE's experience, coordinating capacity building and particularly matching those countries that request assistance to those funders and implementers that can help them, in addition to ensuring those efforts are sustainable and not one-off events, is a very resource intensive process. It would be most impactful for the OEWG to first explore what coordination efforts, mechanisms or platforms exist (including the GFCE) and whether they can be leveraged and supported to achieve the desired results without creating a new structure. This is especially important considering capacity building resources are already scarce and could be used for practical capacity support, rather than spending valuable resources on negotiating the development of new mechanisms and efforts that could potentially duplicate and fragment existing mature initiatives. At the very least, the proposed recommendation to create a new operational capacity building POC, and whether and how such a recommendation is implemented, deserves further study.

Instead, the UN could play an important role now in furthering coordination of capacity building, namely by strengthening existing initiatives and encouraging States to share information on their capacity building efforts and programs while underscoring the potential impact of greater information sharing and transparency. The UN could make such information available on existing platforms, such as the Cybil Portal and Cyber Policy Portal, stressing the need to leverage what already exists for improved consolidation of information. In the GFCE's experience, mapping projects and identifying available resources (such as funding, expertise, etc.) is central to improving coordination. This mapping work enables us to see where the gaps lie and potential areas for better coordination and improvement. The UN could encourage States to provide updates on their capacity building programs and activities, and make this information available on the Cybil Portal. To this end, there could be a dedicated place on the Cybil Portal to make this information more easily accessible if of interest. The UN could also strengthen existing initiatives by encouraging States to participate in mechanisms where coordination is already taking place, such as, inter alia, regional organizations and multistakeholder platforms such as the GFCE.

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

The GFCE's experience of strengthening cyber capacity and supporting access to capacity assistance through a multistakeholder and diverse approach spans over seven years. We have developed and shaped a flexible and dynamic capacity building ecosystem, based on global multistakeholder engagement and collaboration through three "functions" of the GFCE: coordination, knowledge sharing, and match making. Reflecting on the GFCE's structures for knowledge sharing, multistakeholders play a driving role in bringing in perspectives on research, implementation, technical developments and expertise. The private sector and civil society have also become increasingly active in suggesting realistic and pragmatic steps for safeguarding a peaceful cyberspace. We would like to share some examples of the role stakeholders play in the GFCE ecosystem that has worked well:

GFCE Working Groups

The GFCE's multistakeholder community come together to share, shape and form knowledge on specific issues in thematic Working Groups. By pooling the knowledge of the Community, the GFCE has produced several good practice documents, guides and tools that can be used as free resources to improve cyber capacity and to support capacity building actors with implementation of activities. The Working Group on Cybersecurity Policy and Strategy has produced an Activity Catalog on National Cybersecurity Strategy Design ("Catalog") which identifies 20 activities that could go into a project that supports a country in their NCS development journey. Over 15 stakeholders from the GFCE network contributed to the development of the Catalog, and the Catalog in turn informs countries on the types of capacity support available from the GFCE network. Besides top tips and case studies, the Catalog reveals the role stakeholders play in supporting a range of capacity building activities in the NCS development cycle. For example, if you require support on involving relevant stakeholders in the NCS development and implementation process, which ensures better informed and evidence-based policy outcomes, Global Partners Digital and the Organization of American States have experience and expertise in implementing such projects. The Catalog is a fantastic example of how a multistakeholder network can work together, to pool their knowledge and expertise into a practical tool, while demonstrating their role as implementers in the delivery of capacity building assistance.

Global Cyber Capacity Building Research Agenda

Within the Working Groups, the community identifies knowledge gaps and prioritizes them, resulting in the development of a bi-annual Global Capacity Building Research Agenda. Four research projects have already been concluded through this mechanism, effectively engaging the broader Academic Community to address cyber capacity knowledge gaps, identified by the global community in their discussions on challenges towards developing their own capacity. Of relevance to discussions on responsible state behavior in cyberspace is, for example, the research project on cyber norms implementation ("Putting Cyber Norms in Practice") which looks at national examples from across the world to illustrate how norms can be implemented in various national contexts and formats. The academic community, as authors of the research reports and as members of the GFCE Research Committee, supports capacity building in this regard by providing data, evidence and analysis and research generated through the mechanism seek to support informed practical and policy capacity solutions.

Cybil Portal

Another important tool that the GFCE Community has developed is the Cybil Portal – a global, open and free knowledge repository with information on over 800 cyber capacity projects, and nearly 300 tools and resources, and more. Cybil contributes to stronger global cyber security and cybercrime capacity by helping capacity building projects to be more effective – through accessibility on information and improving transparency. Information and updates for the portal is primarily provided by the multistakeholder GFCE Community, they also provide feedback for improvement and suggest the addition of new features. The contributions of the multistakeholder community include updates on projects that they are implementing or supporting (ranging from the establishment of CERTs to delivering cybercrime training), new tools or reports that they have been developed, and webinars or events they are organizing. Effective capacity building does not happen in isolation with governments and requires cooperation and engagement of other stakeholders. This too is reflected on Cybil, only 40% of actors listed on the Cybil Portal are States or government actors. The contributions of stakeholders to the development and relevance of the Cybil Portal are particularly useful and important for effective capacity building coordination efforts. As the portal maintains an overview on capacity building projects and programs to understand who is doing what where, the GFCE uses the data to produce regional coordination notes and organize coordination meetings to connect actors. Through this, we can identify where the gaps are as well as potential areas for better coordination or cooperation.

Clearing House function

The GFCE's role in coordinating offers and requests for capacity building support as a "match-maker" is made possible due to its multistakeholder network and availability of project information through the efforts of the Cybil Portal. The GFCE has supported Tunisia, Sierra Leone, Senegal and The Gambia with specific capacity building requests. The Gambia received support from the GFCE Working Group on Cybercrime, utilizing extensive knowledge and expertise within the multistakeholder group to develop national data protection and cybercrime legislation. In our experience, stakeholders with relevant expertise and knowledge have responded enthusiastically to clearing house requests. The GFCE in turn provides a space for international implementing partners to connect with the recipient country to accurately identify their capacity needs and connect with others working in the country/region to avoid duplication and ensure efficient use of resources. With the establishment of GFCE Regional Offices and designation of Regional Liaisons over the last two years, the GFCE is increasingly well-positioned to support regional actors in CCB in the process to accurately identify needs, define a regional agenda and bring this to the global Community to address – bolstering its demand-driven approach. It also ensures local stakeholder involvement which is important for local ownership and sustainability.

It has been fruitful for us to create an ecosystem that supports the community to share information on their projects, lessons learned, good practices and encourage transparency to build trust and support one another in the process. Given the GFCE's ecosystem and multi-stakeholder network, the GFCE is well-suited to support and implement capacity building measures agreed at the OEWG. We highlight the GFCE's commitment to work with the UN and others, and to support in any way that we can. To this end, we will continue to put forth the GFCE platform as THE platform for international cyber capacity building and look forward to continued work with the UN, member states and other stakeholders to make cyber capacity building more available, more effective and more coordinated.