Informal Multistakeholder Cyber Dialogue

CYBER POLICY CAPACITY BUILDING SESSION
8 December 2020
SESSION REPORT

GENERAL SUMMARY

The discussions in the OEWG to date have reaffirmed the role of cyber capacity-building (CCB) in addressing the systemic, transnational risks and vulnerabilities associated with the digital transition, the lack of ICT security, disconnected technical and policy capacities at the national level, as well as the associated challenge of digital inequalities. States have also noted that in addition to technical skills, there is a pressing need for building expertise across a range of diplomatic, policy, legislative and regulatory areas.

The main objective of the session was to dissect problems, needs, and ways forward to achieve meaningful participation of all countries involved in discussions on disarmament, peace, and stability in cyberspace. Building on the agreement that "*International cooperation and assistance can play an essential role in enabling States to secure ICTs and ensure their peaceful use*"[1], the session unpacked problems, needs, and way forward of this engagement[2]. Some of the issues at stake include prioritisation based on needs assessments, the focus on policy in CCB, the identification of mechanisms for the sustainability of funding and skills transfer, the development of impact metrics, and the nexus between development and security.

In order to ensure balanced perspectives, the session included speakers from Morocco, South Africa, Nigeria, the EU, India, Brazil, the UK, and Australia. The Co-Chairs also shared a resource pack of cyber capacity building initiatives on policy across the world prepared in cooperation with the Global Forum on Cyber Expertise (GFCE) and invited Member States and other stakeholders to add to these initiatives and to increase commitments to what exist. The resource pack is available at the conference website: www.letstalkcyber.org. The session attracted a broad participation of 271 people who joined the event from Zoom and the Livecast. The Livecast attracted viewers from 23 countries and 33 cities around the world.

SESSION OUTLINE

Many of the ongoing efforts undertaken globally focus on strengthening and delivering technical, institutional and legislative capacities. However, while international partnerships and cooperation are often recognised as a key element in the national or regional cybersecurity strategies or policy frameworks, this aspect has been so far neglected in the international approaches to cyber capacity building. The limited capacity of certain parts of government to

[1] UNGA (2015:10). A/70/174

[2] See objectives and guiding questions of the session in the concept note available at https://eu-iss.s3.eu-central-1.amazonaws.com/horizon/assets/BpIVojEd/concept-paper-ccb-final.pdf

fully participate in international cyber policy discussions creates an obstacle for governments to fully embrace whole-of-government and whole-of-society approaches, on the one hand, and limits their capacity to represent their country's positions, on the other hand. The session reiterated the importance of representation, local ownership, and evidence-based strategic objectives and goals.

Part I: Designing an inclusive CCB agenda: issues, interests and priorities

1. The session enquired on whether thinking about CCB in terms of the best practice paradigm was optimal as these cyber security best practices might not be applicable to a variety of national contexts. Nevertheless, the session highlighted certain principles such as the diversity of stakeholders and the important role of the private sector, the need for research to measure impact, and the inclusion of the sustainable development goals.
2. The 2030 sustainable development goals (SDGs) were emphasised considerably, in particular goal 4 on inclusive and equitable education and the promotion of lifelong learning for all and goal 5 on achieving gender equality and empowerment for all women and girls receiving the top spot. Several speakers agreed on the need to encourage Member States to mainstream the SDGs in all UN discussions. The session recognised also that the inclusion of language on SDGs within the First Committee mandating resolutions was an indication that the whole of UN approach embracing all the pillars of human rights, security and development should be applied also to CCB.
3. The session acknowledged the disproportionate attention given to technical issues related to cybersecurity. The participants agreed that there is a need to bridge technical CCB and policy by also educating the technical community on the policy issues and vice-versa. To this end both technical and policy communities must establish ways of engaging and setting CCB priorities.

Part II: Moving towards a more balanced CCB agenda: state of play and possible pathways

4. The session focused on the donor, implementer and beneficiary relationship. It highlighted the importance of local ownership of capacity building even extending to medium of instruction. Language was recognised as an important aspect and this issue was highlighted by the fact that as countries develop National Cybersecurity Strategies, these only serve the purpose of building trust and transparency when they are understood globally which means the use of common concepts and the need for translation into certain languages, often English. There should also be more efforts by implementers and donors to develop and implement CCB activities in other languages and create resources in those languages too to help with the establishment of a common baseline and understanding of key principles.
5. For countries that do cyber capacity building independently, domestically and regionally, partnerships should be able to meet them where they need and sometimes it is in translation services. A comprehensive set of CCB initiatives and services on offer should reflect this principle.
6. Priorities of Member States for cyber capacity building differ and the session highlighted that these have more to do with the local realities than global narratives and likewise, CCB

stakeholders respond more to the local needs rather than to global principles. At the core of all, capacity building relationships are based on trust and partners should not seek to expedite programmes at the expense of building trust which can be harnessed and nurtured over a long period of time.

7. The session highlighted the need to increase transparency at the implementation level by drawing from local expertise so that on the one hand, cyber capacity building goes beyond one-off workshops and interventions; on the other, financial resources circulate in the beneficiary countries as well. This triangular level of relationship of donor, implementer, beneficiary contributes to building trust, accountability and sustainability. The session highlighted how sustainable, strategic and long-term funding can be instrumental to these efforts. One that is also flexible where needed and open to an appropriate mix of mechanisms, including modalities and selection procedures.
8. The important concept of responsible solidarity as the idea of mutually agreed partnership goals and capacity building priorities emerged. The session also highlighted the need for this solidarity or partnership to be approached as a process and not an event and in this regard, the relationship should begin even at the scoping phase to identify gaps and solutions.
9. The issue of differing priorities between donor and beneficiary was discussed, and peculiarities in different regions. Speakers suggested that a baseline of principles should be part of the relationship and these include the respect for human rights, freedom and participation of civil society amongst others. The key reference in terms of a partners' commitment to these priorities are accessions to various UN and regional Conventions and Protocols.
10. In the spirit of politically neutral capacity building, participants raised the issue of the need for a more contextualized approach to capacity building when linked to specific legal instruments or conventions, especially when certain conditionality is attached. While these are some of the ways to achieve harmonisation across a policy area, it is important to better explore the trade-offs that such approaches to policy capacity building create.

Part III: The world of 100% capacity: is the international community ready?

11. The primary question raised during the session was whether the future CCB efforts should focus on strengthening capacities for the implementation of the provisions in the OEWG and UNGGE reports or whether it should rather focus on strengthening the capacity of the recipient countries to be more independent actors in the future discussions. Speakers noted that the OEWG draft pre-report does not give a clear answer in this regard and includes a double objective: a) to support states in adhering to their international commitments and creating resilient, secure and peaceful ICT environment; and b) in order to support states in developing their own understandings of international law, norms, etc.
12. Regarding the need for capacity building partnerships that reflect nationally identified needs and priorities, the discussion revealed that while some efforts might be perceived as insufficiently reflecting the local needs, many countries consider the conversation to be driven by different groups. Participants reinforced that the direction and substance of CCB is being shaped by all Member States. For instance, it was highlighted that some countries from the global South actively participated in the past three GGEs and provided

substantive input with the global South in mind.

13. The session agreed that achieving full cyber capacities is an ambitious goal that is hardly possible to achieve given the speed of technological innovation and evolution of the threat landscape. This challenge is equally valid for all countries independently on the stage of their development.
14. It was clearly recognized that the OEWG provided a platform for Member States that had previously been absent from the global discussions about cyberstability and responsible behaviour in cyberspace. The key take-away was that more voices will strengthen the accountability and transparency of the whole system.
15. Several speakers have stressed the role that regional organisations play in delivering cyber policy capacity, in particular through convening the right actors, ensuring more contextualized support and strengthening the local ownership dimension. However, their role is often hindered by the fact that the mandates reflect all Member States' maturity. Member States determine how fast or slow regional organisations should take up the role of CCB. The session also highlighted that while the global UN discussions may move at a certain pace, regional organisations interface closer with Member States and are able to move at the pace wherein no Member State is left behind.
16. While we 'wait for 100% capacity', there is a need to reflect on CCB priorities and how they evolve, in particular to ensure that the initial objectives and developmental goals are not undermined by more short-term policy considerations. In this, the research community will play an important role as part of the multi-stakeholder community in the OEWG and in CCB discussions.

MAJOR THEMES/AREAS OF CONVERGENCE

a) CCB and ICT related capacity building priorities have evolved since the early 2000s. It is important to understand how and why these changes occurred and what is their impact on the global cyber capacity efforts.
b) CCB are not once-off initiatives but rather a continuous and sustained endeavor and an integral part of National Cyber Strategies and of their reviews.
c) The 2030 sustainable development goals are key areas for cyber capacity building in the context of international security. A special focus must be paid to SDGs 4 and 5.
d) Member States should shift attention to capacity building on policy issues by bridging gaps between technical and policy communities
e) The relationship between donor, implementer and beneficiary to deliver cyber capacity building should be based on trust and transparency.
f) Local ownership of cyber capacity building is important for sustainability. This includes skills transfer for local implementation of CCB programmes and funding management.
g) Cyber capacity building programmes like development and sharing of National Cyber Security Strategies only serve the purpose of building trust when they are widely understood in a common language. Translation of Strategies into UN official languages and their publication in UN Platforms is a substantive and administrative priority.
h) Despite divergences and peculiarities on CCB priorities, the respect for human rights and participation of civil society must form the basis of partnerships.