Cyber policy capacity building agenda

A session co-chaired by the Department of International Relations and Cooperation of the Republic of South Africa, EU Institute for Security Studies, Research ICT Africa

8 December 2020
12:00 – 15:00 UTC
13:00 – 16:00 CET
14:00 – 17:00 SAST

CO-CHAIRS CONCEPT NOTE

Rationale and objectives

The discussions in the OEWG to date have reaffirmed the role of cyber capacity-building 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.

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 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 main objective of the session is to dissect problems, needs, and ways forward to achieve meaningful participation of all countries involved in discussions on disarmament, peace, and stability in cyberspace.

The session will aim to answer the following questions:

1. How can the international community contribute to strengthening national and regional capacities in order to participate in the international processes on cyber issues?

2. How can the international community implement cyber capacity building that supports the whole-of-government approach in international cooperation?

3. Considering that donor and recipient countries might have different priorities and objectives, how can we ensure a more representative cyber policy capacity building agenda that reflects a broad list of priorities such as norms and international law but also economic growth and human development?

Format

To facilitate debate across the three sub-themes identified below, the session is organised in three parts. First, a Welcome Note from the Session Chair, who will provide a contextualisation of the CCB in the First Committee in the international peace and security framework. Our speakers and discussants will then take the floor to introduce each of the sub-themes, before inviting other participants to offer input and contribute to the debate.

We kindly ask participants interested in contributing to the discussion to contact the co-chairs ahead of time.

This session is also an opportunity to map the existing resources for policy-related capacity building efforts. A resource pack prepared by the co-chairs will be uploaded to the event's website, and will cover the following areas:

1) **Policies**: mapping of the efforts aimed at addressing cyber policy capacity building in relation to responsible state behaviour in cyberspace;
2) **Institutions**: mapping of the institutions active in cyber policy capacity building;
3) **Resources**: mapping of funding mechanisms and instruments for cyber policy capacity building.

Countries, institutions and organisations active in not-for-profit cyber policy capacity building are invited to flag such initiatives to the co-chairs of the session.

Agenda

12:00 – 12:05 UTC
Welcome and opening remarks

12:05 - 13:00 UTC
Designing an inclusive cyber capacity building agenda: issues, interests and priorities

Since the 2013 UNGGE report, the international community has invested significant resources in strengthening technical capacity building i.e. how to set up institutional arrangements to fight cybercrime, including CERTS, develop national legislation on cybersecurity and cybercrime, or strengthen international cooperation through the points of contact.

While technical structures and processes are necessary to tackle cyber threats and attacks, there is an increasing recognition of the need to strengthen human capacities on cyber policy and digital diplomacy, that would deliver a more inclusive and representative participation in the international security debates. This is particularly true for the ongoing multilateral processes at the United Nations where cyber capacity building is at the core of conversations about norms, international law and confidence-building measures. Perceived primarily as a North-to-South conversation, cyber capacity building discussions often fail to adequately reflect considerations and interests of countries in the South.

This session aims at problematising and unpacking problems related to cyber policy capacity, to reflect whether current cyber capacity initiatives account for the complexities and challenges faced by developing countries. Some of the issues that will be highlighted during the session include inclusiveness of women and other underrepresented groups in cyber policy capacity building, lack of specialised education programmes in cyber policy, and difficulties to design, resource, and sustain capacity building programmes on cyber policy and diplomacy.

Chair	Moliehi Makumane, Department of International Relations and Cooperation, South Africa
Scene-setter	Enrico Calandro, Research ICT Africa
Speakers	Elizabeth Kolade, Nigeria
	Asoke Mukerji, Distinguished Fellow, VIF, India

13:05 – 14:00 UTC

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

It has become the norm to expect a country to adopt a national cybersecurity strategy or an equivalent policy framework. Where such strategies or frameworks are in place, the focus of capacity building initiatives is primarily on the technical aspects and rarely on the international cooperation aspects of the strategies.

Only a fully inclusive and transparent international debate that promotes and ensures meaningful, gender-balanced, and competent participation of all stakeholders can deliver a sustainable and legitimate outcome. This is also true for peace and trust in cyberspace.

However, capacity building needs to be funded and when domestic resources run short, external partners offer to and are invited in to provide the CCB. How do we make the conversation between the 'donor, implementer and beneficiary' reflective of everyone's priorities including primarily for the beneficiary, to build meaningful cyber policy capacities that reflects a whole-of-government and whole-of-society approaches and is locally informed?

Some states are already taking active measures to increase policy capacity globally through various mechanisms:

1. Institutional (e.g. specific cyber policy related curricula for the training institutions such as national schools of administration or diplomatic academies, funding for the training programmes and fellowships);
2. Policy (e.g. a conscious effort to increase the level of competence across government and society);
3. Strategy (e.g. focus on international cyber engagement in national cybersecurity strategy, including adequate resources), or through public-private partnerships.

The session will take stock of these initiatives but also aim to answer how they fit within a broader spectrum of priorities of the recipient countries (e.g. development) and to strengthen the engagement between donors, implementers and beneficiaries.

Chair	Moliehi Makumane, Department of International Relations and Cooperation, South Africa
Scene-setter	Joyce Hakmeh, Chatham House
Speakers	Claudio Leopoldino, Ministry of Foreign Affairs, Brazil Marwa Azelmat, Association for Progressive Communications, Morocco

14:05 – 15:00 UTC

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

At the end of the session, we will critically look into the future. It is a well-established fact that national government entities and agencies do not always have the adequate capacities needed to participate substantially in the ongoing debates or observe emerging norms, rules, and principles on responsible state behaviour, or to achieve gender balance in these processes.

On the other hand, cyber capacity building is also an instrument to advance values, positions and agendas on international cyber security. As a policy instrument, capacity building is not apolitical, considering that donor and recipient countries might have different priorities and objectives. Therefore, the tone of the conversation about cyber capacity building needs to strike a balance between the North and South agendas.

As more developed countries enter the donor field of cyber capacity building, the socialization process is in part aimed at getting more UN Member States participating substantially in the UN processes and in part at sharing and exchanging views on the current debates. As more countries attain the capacity to develop national positions on all five areas of the debate i.e norms, threats, international law, the question arises whether the current institutions are fit for a 'cyber dream' whereby states develop significant levels of capacity, which in turn emboldens them to take more independent stances in international negotiations. Participants will also discuss how to strengthen and improve South-South and North-South mechanisms of policy-related cyber capacity building – for instance, through public-private partnerships, regional and global coordination, international cooperation, and national strategies inclusive of cyber policy capacity.

Chair	Moliehi Makumane, Department of International Relations and Cooperation, South Africa
Scene-setter	Patryk Pawlak, EU Institute for Security Studies
Speakers	Briony Whitaker, Department of Foreign Affairs and Trade, Australia Kerry-Ann Barrett, Organization of American States