Informal Multi-stakeholder Cyber Dialogue

CONFIDENCE-BUILDING MEASURES (CBMs)
10 December 2020
SESSION REPORT

GENERAL SUMMARY

The session attracted a broad participation of 148 people who joined the event from Zoom and the Livecast. The Livecast attracted viewers from 15 countries and 20 cities around the world.

SESSION OUTLINE

The session opened with an introduction by the moderator Mila Francisco of Chile, who summarised the rules of the discussion as well as the central themes of the session, introducing the main questions and topics for the session:

- *How do regional organizations approach the development in implementation of CBMs at the regional level? What are the fundamental similarities and differences?*
- *What did the Organisation for Security and Co-operation in Europe (OSCE) and the Organisation of American States (OAS) deliver in terms of CBM implementation and cross-regional information exchanges? Views of non-governmental stakeholders.*
- *With respect to the draft "CBM" section of the OEWG pre-draft report (points 45-52), are there any notable omissions, or statements with which you disagree? The role of non-state actors, NGOs, tech companies, etc. in the implementation of CBMs, the outreach activity of international organizations towards them.*

Péter Tamás Horváth of Hungary started the presentations, providing some scene-setting and highlighting the main activities of participating states at the OSCE in developing and implementing CBMs. The informal working group on cyber issues of the OSCE was established to develop consensus on CBMs, to enhance cooperation, transparency, predictability and stability in state relations, and reduce the risk of escalation and misperception, continuing the successful work on CBMs for conventional conflict. OSCE's CBMs call for responsible state behaviour in the use of ICTs, dealing with transparency, communication, and national preparedness to address cyber challenges. Multi-stakeholder participation is encouraged at the OSCE, with key events gathering diverse non-governmental stakeholders. The OSCE is also a testing ground for new ideas, such as the "Adopt a CBM" initiative.

Szilvia Toth, from the OSCE Secretariat, reinforced the history of the OSCE creating instances for cooperation around confidence-building measures, as well as cooperation with regional organisations. Emphasis is placed on implementing CBMs. Although the OSCE engages in cyber issues in a working group with government representatives, other stakeholders are regularly invited to present on topics related to on CBMs implementation. Efforts include workshops and trainings, involving non-governmental stakeholders, which allows a wider perspective and exchange with government representatives. OSCE CBMs encourage participating states to engage with stakeholders and national structures.

Pablo Castro, from Chile, emphasised the history at the OAS of confidence and security building measures as an important tool promoting peace, building trust and enhancing cooperation. A natural step forward in this historical process is the creation of CBMs in cyberspace, and Inter-American dialogue allowed for a common cybersecurity strategy. The OAS working group on cooperation and CBMs in cyberspace was established with the mandate to draft CBMs based on the consensus UN GGE 2015 report, with recommendations that have included providing information on cybersecurity policy; designating national points of contact at the policy level; and strengthening and promoting cyber diplomacy. The latter responds to a need of engagement of Foreign Affairs Ministries in cyber discussions. Challenges remain on implementation, linkage to other issues such as norm implementation and the application of international law, and gender considerations in cyber policy. Non-governmental stakeholders are engaged at the OAS level, and can play different, important roles at the national and international levels. Lessons can be gathered from other regional organisations as well.

Louise Marie Hurel, from Igarapé Institute first provided an overview of the changing and expanding nature of CBMs, looking at them broadly in the context of a changing discussion on CBMs from conventional conflict to cyberspace, and highlighting the cross-pollination happening between different initiatives; also, a shift in focus from the context of traditional disarmament and arms control, with questions of peace and stability seen through the challenges of cyberspace, and the difficulty to separate the national/regional/international levels. Focus was brought to the convergence between confidence, cooperation and coordination**.** Non-governmental stakeholder engagement requires not only attending discussions, but working together at the national and regional level, bridging the gaps between different kinds of knowledge, and consolidating views. Non-state actors can help in specific elements: ensuring there is a rights-respecting and gender-sensitive lens in the formulation or implementation of CBMs and enhancing capacities for implementation of the CBMs. Good practices can be improved too, for instance, to consolidate points of contact designated for specific agendas, like critical infrastructure, cybercrime, etcetera, to flesh out different dimensions of CBM implementation.

Finally, Andraz Kastelic, from UNIDIR, presented the Cyber Policy Portal: a confidence building tool developed in 2019, as an interactive online tool providing information on cybersecurity policy by UN member states. As such, it promotes transparency and facilitates information exchange and capacity; by doing so it attempts to dispel ambiguities and reduce tensions among nations in cyberspace. It is aimed at diplomats, policymakers, and security policy experts.

The interventions were followed by an open discussion. Participants and panellists discussed the role and the value of CBMs in practice, their importance in the context of attribution of cyber incidents, and good practices in communication between different stakeholders such as diplomats and CSIRTs. Closing remarks by J. Carlos Lara of Derechos Digitales emphasised takeaways regarding effectiveness of CBMs, the need for inclusiveness in their development and evaluation, and the need for further discussion and encouragement in international forums, including in the context of the OEWG.

MAJOR THEMES / AREAS OF CONVERGENCE

- *Implementation as the priority challenge.* Implementation remains a common challenge, and though there seems to be a lack of appetite to develop new CBMs, there seems to be consensus that meaningful implementation of known CBMs is crucial. There needs to be a more honest conversation between state representatives on how to implement already recommended CBMs.
- *Regional organisations play an important role in norms implementation.* Regional organisations have manifested their intention to develop and implement CBMs as a major driving force for multi-level efforts to build trust among states and non-state actors. Regional organisations play an important role in translating CBMs into practice, including through information exchange, capacity building, and gathering of best practices. At the same time, dialogue between different regional organisations, as well as complementary dialogue at the global level, can support CBM adoption.
- *Following up is a key element of implementation.* CBMs allow the conditions for principles, rules and norms to function in practice. But to understand whether they can serve their purpose in the event of an attack or crisis related to ICTs, their implementation must be monitored and independently evaluated. Otherwise, cooperation and procedures to deal with cybersecurity crises can fall short on their promises to generate trust and prevent escalation in case of incidents.
- *CBMs are complementary to other efforts, especially capacity building.* CBM implementation goes hand in hand with capacity building. Capacity building also creates buy-in and ownership from participating states and allows for meaningful discussion of CBMs between state representatives. It ensures that what ministers agree in meetings is translated into action, making sure countries have capacities and resources to maintain commitment to implement CBMs, and incorporating rights-respecting and gender-sensitive perspectives.
- *Taking stock of existing CBMs*. Confidence building measures have been highlighted and reported before, but there is a need to map these mechanisms because states and non-state actors need to know what is available and what is already in place, ensuring that there is no overlap of mechanisms, that the mechanisms and channels that are available are used, and that there is interpersonal trust at different levels. Good practices such the informal daily communications between CSIRTs, also represent trust-building activities that need to be highlighted.
- *The role of non-state actors.* In different national and regional initiatives, non-governmental stakeholders are actively involved in the discussions on how to implement

CBMs. Non-governmental stakeholders can play key roles in capacity building, as well as in the design, implementation, monitoring and evaluation of CBMs.

- *The impact of building trust.* The repercussions of large-scale cyberattacks affect states, but also individuals and other sectors. Trust is transversal and requires an approach that considers the impact of cyberattacks in the implementation of CBMs. Trust must be built also with all possibly affected individuals and groups as well.

RECOMMENDATIONS

- States and international and regional organisations should maintain and build upon efforts for implementation of existing confidence-building measures. States should also consider monitoring and evaluation mechanisms to follow up implementation.
- States and international and regional organisations should maintain and build upon regular information exchange as a confidence-building mechanism, utilising the forums already in place and engaging with different stakeholders. States should endeavour to map and learn about measures that are already present in other countries and regions, as well as the best current practices of non-governmental stakeholders.
- States should prioritise mechanisms to support implementation of known confidence-building measures involving non-governmental stakeholders.
- States and regional organisations should endeavour to engage in more inter-regional dialogue for all CBM processes, not just on cyberspace, to prevent escalation of conflicts. States should accordingly clarify the roles and expertise of different representatives, while allowing meaningful dialogue between different forms of expertise.
- The OEWG report should include reference to the role of non-governmental stakeholders, including civil society, academia, the technical community and industry, in supporting the implementation of norms, rules and principles. The OEWG report can be expanded with a reference to CBMs developed by States that require the involvement of the private sector to be fully operationalised.
- Existing mechanisms that involve non-state actors should be expanded to include stakeholders currently not participating in discussions, in order to improve states’ capacity to integrate different rights-respecting perspectives in the adoption of measures to build trust with other states as well as other stakeholders.