Working-Paper to advance the ongoing Discussions within the United Nations Open Ended Working Group (OEWG) on Confidence Building Measures (CBM) in Cyberspace

Introduction

Cyberspace and more concretely ICTs offer immense opportunities for social and economic development. At the same time, the worldwide increase in reliance on digital technologies comes with increased risks of malicious cyber activities that may undermine international peace and security. Given the global nature of the threats faced by UN member states it is crucial to step up international cooperation and confidence-building to foster trust, cooperation, transparency and predictability.

Confidence Building Measures (CBMs) are a well-proven and established tool in international relations to promote peaceful uses, transparency, stability and to help reduce the risk of misunderstanding, escalation and conflict. They can contribute to defusing tensions and can serve to guide States’ behavior resulting in more stable international relations. In cyberspace, the potential deniability, potency and low cost of malicious cyber activities add to the need for CBMs that are specifically tailored to the cyber context.

Building confidence is a long-term and progressive commitment requiring the sustained engagement of States. Therefore, this working paper, submitted jointly by Australia, Brazil Canada, Germany, Israel, the Republic of Korea, Mexico, the Netherlands and Singapore, who have formed an informal, open, cross-regional group to advance CBMs through the work of the Open-Ended Working Group on security of and in the use of information and communications technologies 2021-2025 (OEWG), aims at underlining the need for progress in implementing and agreeing to cyber CBMs at the UN level through providing concrete input for the ongoing discussions within the OEWG process with a view to advancing CBMs that can be implemented in a voluntary, non-binding manner by all UN member states.

Confidence Building Measures at the regional level

Regional and sub-regional organizations have made significant efforts in developing CBMs, adapting them to their specific contexts and priorities, raising awareness and sharing information among their members. The continuous work of States on CBMs in different regional formats shows that in principle, States are willing to develop, deepen and put into action a comprehensive set of CBMs.

Concrete regional initiatives, undertaken inter alia by the Association of Southeast Asian Nations (ASEAN), the Organization of American States (OAS) or the Organization for Security and Cooperation in Europe (OSCE), on the adoption and implementation of suitable CBMs can serve as potential models for CBMs at the UN level. The regional initiatives can also substantially contribute to put into practice the CBMs agreed by the UN. We welcome views and lessons learned from all relevant regional and sub-regional organizations, as well as their participation in this work going forward. More inter-regional dialogues and sharing of experiences could be promoted within the UN framework.

CBMs that have been implemented successfully at a regional level can be considered for establishment as CBMs at the UN level. Regional organizations could facilitate the process of working out CBMs in the OEWG by providing experiences on successful CBMs and demonstrating that far-reaching CBMs are possible.
Confidence Building Measures at the UN level

Stepping up efforts to advance CBMs at the UN level is key to enhancing global cyber-security while also ensuring that States that are not part of a regional network are not left out.

Within the UN, substantial progress has been made over the years to develop CBMs for cyberspace. These efforts have been undertaken inter alia by the United Nations Groups of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (UN GGEs) and the 2019-2021 OEWG. The OEWG-Report A/75/816 and GGE-Reports A/68/98, A/70/174, and A/76/135 provide valuable input and present CBMs covering the implementation of norms, the integrity of supply chains, dialogue, transparency and information sharing, points of contact, training and other measures which at the same time can contribute to bridging capacity gaps.

Further work is needed to enhance the scope and the operationalization of CBMs at the UN level. Work is also needed in view of better identifying and reporting obstacles to the implementation of the CBMs and linking these to existing capacity building opportunities and needs.

To facilitate the implementation of CBMs, States, supported by other stakeholders as appropriate, should engage in international cooperation and capacity-building, based on the principles for capacity-building contained in the 2021 OEWG report.

The OEWG is the key framework to promote CBMs at the UN-level. This non-paper strives to provide practical input for the OEWG process with a view to advancing CBMs that can be put into action and can be operationalized by all states.

Proposals for the upcoming OEWG sessions

Without ruling out other alternatives and building on the recommendations made by the reports of the UN GGEs and the OEWG, the following CBMs are considered suitable for elaboration within the upcoming OEWG sessions in order to advance CBMs at the UN-level:

- Creating, implementing and specifying the purpose and organizational details of a global network of Points of Contact (PoC). Such a network could be a helpful first step that would facilitate the use of other CBMs. A suitable starting point could be identifying or appointing dedicated PoC’s at the policy, diplomatic and technical levels. Where relevant, additional kinds of PoCs may also be established.
  - Regarding the operationalization, a first step should focus on less -complex tasks like guidance on communications checks and joint table top cyber exercises, including scenario planning, in order to subsequently increase the effectiveness of the global network of PoCs once it has been successfully operationalized.
  - With a view to creating inter- and intra-governmental procedures to ensure effective communication between PoCs during crises, standardized templates could be developed to indicate the types of information required, including technical data and the nature of the request. These should be flexible enough to allow for communication, even if some information is unavailable.
  - The functionality and operationalization of this global PoC directory within the UN would require resourcing and could be advanced through more specific recommendations by the OEWG.
  - Meanwhile, States can voluntarily submit their national PoCs as part of their responses to the online self-assessment tool National Survey of Implementation of United Nations recommendations on responsible use of
ICTs by states in the context of international security on UNIDIR’s Cyber Policy Portal (from 1 May 2022). Information regarding PoCs will not be hosted directly on UNIDIR’s Cyber Policy Portal for security, but will be collated by UNIDIR and distributed to participating States on a regular basis (biannually).

- Sharing and dissemination of information and good practices on establishing and sustaining national Computer Emergency Response Teams (CERTs) / Computer Security Incident Response Teams (CSIRTs) and on incident management.

- Enhancing the scope of information sharing is key for building international trust. One aspect is the voluntary exchange of information, where applicable regarding national cyber doctrines, cyber capabilities and the existence of checks and balances without revealing confidential information. One other aspect could be sharing national efforts on gender perspectives in cyber security.

- Voluntary sharing of information and good practices, lessons or white papers on ICT security-related threats and incidents, national strategies and standards for vulnerability analysis of ICT products, national and regional approaches to risk management and conflict prevention, data protection, protection of ICT-enabled critical infrastructure, ICT-security agency mission and functions as well as ICT strategy, legal and oversight regimes under which they operate.

- Foster dialogue through bilateral, sub-regional, regional and multilateral consultation and engagement including, when appropriate, multiple stakeholders. The private sector, academia, civil society and the technical community can contribute significantly to facilitating such consultations and engagement also with a focus on gender equality and diversity.

- Enhance cooperation with the private sector, including with the aim of ensuring the integrity of supply chains and, inter alia, via the development of objective cooperative measures, so that end users can have confidence in the security of ICT products; seek to prevent the malicious uses of ICT tools and techniques and the use of harmful hidden functions; and encourage the responsible reporting of vulnerabilities.