GLOBAL CYBER SECURITY COOPERATION PORTAL

CONCEPT NOTE

Deliberations at the Group of Governmental Experts on the developments in the field of Information and Telecommunications in the context of international security resulted in framing rules, norms and principles for responsible State behaviour in cyberspace, which were adopted by the UN General Assembly through its resolution 71/28. The open Ended Working Group 2019-2021, which continued discussions on the subject and its various related themes, adopted a final report recommending that these perspectives should be further considered in future UN processes on this subject.

OEWG 2021-2025

While deliberations on the normative framework of State behaviour in cyberspace and the developments in the field of ICT in the context of international security continue in the Open Ended Working Group on security of and in the use of information and communications technologies 2021–2025 (OEWG), established pursuant to General Assembly resolution 75/240, there is an underlying need for the OEWG to focus also on concrete ideas that can help achieve the common objective of free, open, secure, stable, accessible cyberspace and its use for peaceful purposes.

During the First and Second substantive sessions of the OEWG, member states have put forward such ideas, especially in the capacity building and confidence building measures, for further consideration of the Group. The development of a “Global Cybersecurity Cooperation Portal” (GCSCP), anchored at the United Nations, as a global platform for co-operation and coordination by member states on cyber issues is one such idea.

Objectives GCSCP:

Currently, there are various bilateral, sub-regional, regional mechanisms for exchange of information and coordination among cyber agencies of member states. However, there is no global platform, which enables such an exchange. Establishment of GCSCP will overcome this lacunae.

GCSCP is envisaged as a one-stop platform for enabling global cooperation and coordination between member states on matters related to cyber security. The portal
can incorporate various components, some of which are currently being discussed by the OEWG.

Management of GCSCP:

GCSCP will be a member state driven portal with the UN Secretariat handling its overall maintenance and management. Each member state will be provided dedicated access credentials by the UN secretariat. Member States can upload information under the various sections of the portal on a voluntary basis. UN bodies, regional organisations and other relevant stakeholders can also share information with UN Secretariat (UNODA) for uploading into the portal.

Content of GCSCP:

The GCSCP will provide the base platform on which various ideas to cyber security discussed under the OEWG can be implemented through a modular approach. GCSCP will have different modules on areas like capacity building, policy frameworks, cyber threats etc, which can be developed independent of each other. It can also integrate best practices under existing national, regional and plurilateral cyber cooperation platforms.

A suggested non-exhaustive list of content that the GCSCP can encompass and their utility is provided below:

- It can be a global repository of information about national cyber security policies, laws, doctrines, regional/ plurilateral frameworks with regards to the use of ICTs in the context of international security.
- It can be a platform for member states for voluntarily sharing and exchanging information on ICT-related vulnerabilities, best practices etc.
- A database of cyber Points of Contact will be incorporated in the platform for facilitating this coordination and information exchange.
- It can serve as an important confidence building measure in the form of a transparency tool that helps in building common understandings and enhancing confidence among States.
- It can incorporate a capacity-building calendar, which will contain information on assistance and capacity building programs offered by member states, UN bodies, regional organisations and other relevant stakeholders.
- It can reflect information on the assistance required by member states in areas related to cyber security. This will enable assistance providers to curate capacity building programs with a focus on specific needs and particularities of recipient State(s).
- A database of assistance Points of Contact can be incorporated in the platform for seeking further information or coordinating capacity building programs.
• It holds the potential to facilitate capacity building of member states.
• The platform can also contain documents related to relevant UN and intergovernmental processes related to ICT security for easy reference for academic research.

Access to GCSCP:

• The portal can incorporate two kinds of content—public and restricted. While public content could be accessible for everyone to view, restricted content could be viewed only by member states. Member states can have the option to choose whether the information they upload or share would be public or restricted information. Information shared by UN bodies, regional organisations and other relevant stakeholders can be public, unless requested otherwise.

How can the OEWG contribute:

The OEWG can recommend the establishment of such a portal to the UN General Assembly. Subsequently, the Group, in its future sessions, can have focused deliberations on the content/modules of the portal for further development.

***