Permanent Mission of India
New York
****

Rev1 Working Paper on Global Cyber Security Cooperation Portal

Table of Contents

Introduction	Page 1
Rationale for the Portal	Page 2
Management of the Portal	Page 2
Module One: Documents Repository	Page 3
Module Two: POC Directory	Page 4
Module Three: Assistance Mapping	Page 4
Module Four:Calendar of Conferences/Workshops	Page 5
Module Five: Incident Information Sharing	Page 6
Stakeholder Engagement	Page 6
Operationalisation of the Portal	Page 7

Introduction

In the context of international security, discussions in the Group of Governmental Experts and the Open-ended working group 2019-2021 on information and telecommunications had focussed on the normative aspects for responsible State behaviour in cyberspace and also on the developments in information and telecommunications. These Groups had also made recommendations to ensure an open, secure, stable, accessible cyberspace and its use for peaceful purposes.

During the deliberations of the OEWG 2021–2025, several delegations have expressed their keen interest in practical and implementable steps that could be undertaken to enhance the security of ICTs and build confidence and trust in the use of ICTs through the OEWG. Accordingly, concrete ideas have also been submitted by member states to the OEWG in the form of concept notes and working papers, which have largely centred around capacity building and confidence building measures, where there is a greater degree of convergence among member states. Member States have often pointed towards having a practical measure that is useful in developing the capacity building for Member States and can have a complementary role to what Member States are doing at domestic level in

enhancing ICTs' security. The First Annual Report adopted by the OEWG by consensus reflects the aspiration of all member states for an action-oriented approach.

The proposal for establishment of a Global Cyber Security Cooperation Portal (GCSCP) is one such practical proposal, which will benefit the member states, especially developing countries.

Rationale for the Portal

GCSCP is envisaged as a one-stop platform for enabling global cooperation and coordination between member states on matters related to ICT security.

Currently, there are multiple portals or webpages related to ICT/ Cyber security with different degrees of usage and efficiency. During the informal inter-sessional meeting in December 2022, many delegations had suggested an online Points of Contact directory, which can be assessed with user credentials. Such an online directory also needs to be anchored in a website/ webpage. As the work in the OEWG matures, many more such proposals could be implemented. From the perspective of small and developing countries and countries that have smaller delegations, accessing multiple platforms and tracking different portals would become excessively time consuming.

The GCSCP is expected to provide an 'integrated' platform for sharing of information, which will enhance cooperation and coordination among member states in the area of ICT security. It will integrate various modules to enhance the security and stability of the ICT space, currently being discussed under the OEWG. The GCSCP Portal is aimed to be a Member-state driven process, with their voluntary participation and sharing of information and relevant documents on ICT security and safety. Such Portal will allow Member States to communicate securely : one-to-one, one-to-many and many-to-many. This will also give opportunity to Regional/Sub-Regional/Existing Capacity Building Initiatives to interact one-to-one on various topics of Cybersecurity. The Portal may become a reliable and collaborative platform under the UN framework for Member States, especially small and developing Member States, for exchanging ICT related information, to be a go-to-destination for understanding latest developments in the global ICT environment, refer to PoCs, share ICT security and safety information and best practices, and initiate a new module based on the Member States' necessity. The Portal, once operationalised, would be a resourceful platform for global capacity building mapping and assistance programs.

Management of the Portal

GCSCP will be a member state driven portal, whereby member states will voluntarily share/ upload the information to the portal. The UN Secretariat will be tasked with handling its overall maintenance and management. Due to its subject expertise and its continuing

support to the inter-governmental cyber process, UNODA is better placed to be the custodian of this portal.

Each member state will be provided dedicated access credentials by UNODA. Member States can access and upload information into the various modules of the portal on a voluntary basis. UN bodies, regional organisations and other relevant stakeholders can also share information related to specific sections of the portal with UNODA for uploading into the portal. Member States may discuss on the portal access modalities for communication in trusted manner. The objective of the Portal to go beyond being an academic exercise of information gathering to developing a global capacity building awareness and mapping of programmes to enhance Member States preparedness in the use of ICTs. Such an active Portal would be an anchor-platform for any future Regular Institutional Dialogue mechanism to rely upon while discussing and developing relevant implementable steps.

Content of Portal

The portal can be implemented through a modular approach, which means that an incremental approach can be taken towards implementing the different components of the portal. Thus, modules can be developed independently, depending on the convergence of views among member states. But since they are mounted on a common platform, they would be able to talk to access the information available in the portal thereby eliminating redundancy.

The portal can incorporate two kinds of content – public and restricted. While public content could be available for everyone who visit the portal, restricted/ private content could be viewed only by member states. Member states will 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.

Modules of the portal

The working paper elaborates below a list of non-exhaustive modules that can be incorporated in the GCSCP.

Module #1: Document repository

Background

From the first GA resolution A/RES/53/70 on 4 January 1999 on ICT security to the recent resolutions in the 77th UNGA, several UN documents on the subject have been generated. These include the consensus reports of the four GGEs, the report of the OEWG 2019-2021, reports of the Secretary-General to the General Assembly, GA resolutions, national statements, working papers, submissions etc. In addition to these documents, several research papers and publications have also been produced by UN bodies and international organisations.

Objective

Despite the availability of vast resources, accessing them is a cumbersome task as they are distributed in multiple platforms. There is no central location where such resources could be easily accessed by member states, especially by small delegations. Creating a repository module can enable quick and easy access of all documents related to ICT security, thereby facilitating the meaningful participation of delegations in future inter-governmental discussions.

Structure

Member states must be able to access or search for resource documents in multiple ways, based on their needs. For example, member states shall have the option of viewing the resources based on their category (reports, statements, research publications etc) or the forum (OEWG, GGE, GA etc). Similarly, there shall also be a provision through which member states could search the contents of all documents in the database. For example, if a member states wants to look up for references to IHL in these documents, the search should be able to retrieve relevant documents.

Module #2: Points of Contact directory

The establishment of a global PoC directory is currently under deliberation of the OEWG. It is pertinent to highlight how the PoC directory is essential to the smooth functioning of the portal as it will help in integration of the other modules. Thus, PoC directory will be the anchor of the portal as every module in the portal will be related to a specific function of a PoC. For example, any uploads/ additions to the 'assistance' modules will specifically trigger the attention of the 'Assistance/ Diplomatic' PoC. This way, the independent modules will be able to share the resources of the PoC directory enabling smooth communication between member states.

PoC Directory's modalities of communication, in particular while interacting with PoCs of regional and sub-regional organizations, would pave way for streamlining information sharing and reporting of cyber incidents to the relevant PoCs.

Module #3: Assistance mapping

Background

Capacity building and assistance has been a topic of discussion from the First GGE on the subject of ICT security. In order to ensure a stable and secure cyberspace, bridging the 'digital divide' would be essential and it can be achieved by pooling resources and sharing knowledge and capacities that exist globally. Bringing together member states, who would need assistance in building their ICT security infrastructure and capacities, and others, who would be in a position to offer such assistance, on a common platform would help bridge this gap.

Objective

The objective of the module would be to create a platform to match the needs of member states with the resources available in the area of ICT security. It will enable the member states to broadcast their assistance requests to a large number of potential assistance providers at one go, which they may be unable to do so presently due to their limited capacities. It will also enable the creation of needs-based programs by potential assistance providers as the assistance needs of member states can be accessed at a central place. It will also help in aggregating resources by organising joint assistance programs for member states, who have similar needs. It will help UNODA also to use the voluntary contributions provided to the Disarmament Trust Fund for support specific assistance needs of member states in ICT security.

Structure

The module should enable member states to submit their assistance/ capacity building requirements through specific templates, to ensure their precise nature. Similarly, member states will also have the option of uploading any specific assistance, which they can offer. The portal itself will acts as an automatic clearing house mechanism of requests and offers. The Portal would be able to provide a broad picture of various assistance building requirements across the globe in various geographies and offer a navigating map for the Member States, regional organisations and the UN on the course of actions needed. Such Portal would complement the role of any future regular institutional dialogue mechanism.

Module #4: Calendar of Conferences/ Workshops

Background

International conferences/ workshops are one of the best environments for sharing of knowledge with a large audience. Given the dynamic and evolving nature of ICT security, cross-fertilization of knowledge through workshops, conferences and seminars are becoming increasingly important. Such events, organised by member states as well as international, regional and sub-regional organisations, and other relevant stakeholders, with the participation of international experts in the field of ICT security, represent excellent opportunity for ICT specialists from member states to participate and enhance their knowledge.

Objective

The module will collate information relating the international conferences and workshops related to ICT security and present this information to member states at a central place. This will enable member states and their specialists to remain updated on any significant international event in the field of ICT security. A global calendar will also help them prioritise their participation in specific areas and depute their specialists.

Structure

The module will have a standard template in which member states will be able to upload information on the ICT security conferences/ workshops organised by them throughout the year. There will be a provision to upload any additional information about the Conference, which the organisers may want to share about their event. The template will

incorporate information regarding relevant nodal points, who can be contacted for further information about the event.

Module #5: Incident Information Sharing

Background

Attacks on ICT systems can have a devastating impact on safety-critical systems, including critical infrastructure. Incidents involving the malicious use of ICTs have increased in scope, scale, severity and sophistication. Due to the differences in capacities and resources, as well as in national law, regulation and practices, global cooperative measures are required to mitigate, investigate or recover from such incidents and reduce vulnerabilities.

Objective

The objective of Incident Information Sharing module is to encourage Member States, voluntarily, to share ICT incidents in a timely manner on the portal for disseminating information that could help prevent any recurrence of similar attacks and alert other Member States on the risks posed by threat actors. Under Incident Information Sharing module, a Member State may also request assistance from others in addressing the challenges to its ICT infrastructure. This module is expected to work in tandem with the rest of the modules and future modules that may be developed in an organic manner.

Structure

Member States may further discuss developing a dedicated template in line with the existing best practices of incident information sharing at the bilateral, regional, sub-regional and multilateral platforms. This template may also provide a mechanism for the Member States to voluntarily share the essential elements of an ICT incident. Through this template, the Member States will also get the opportunity to seek assistance in tackling the ICT incident and at the same time building its capacity to tackle similar future ICT incidents.

Stakeholder engagement

The portal can enable stakeholder engagement with member states in a systematic way. Though it is a member-state driven portal, other stakeholders will have the option to contribute to specific modules by sharing information with UNODA. For example, information on capacity building programs offered by other stakeholders in the area of ICT security can be published in the portal under the ‘assistance’ mapping. International conferences/ seminars vents organised by these stakeholders, which contribute to the current OEWG discussions, can be included in the conference calendar. Stakeholders will be able to view public information shared by the member states in the portal, enabling them to establish direct channel of communication with them.

Operationalisation of the Portal

Focussed discussions within the OEWG on the proposal, including on the contents/ modules that can be part of it would be required before operationalising the portal. Implementing the PoC directory can be a starting point. Other modules like the ‘Document repository’, ‘Conference/workshop calendar’, can also be readily implemented. As the

discussions continue in the OEWG on capacity building, the ‘assistance mapping’ module could be given concrete shape. All these modules can be implemented independently.

Based on the discussions within the OEWG, UNODA could be requested to present an ‘Implementation paper’, which could include the content/ modules of the portal, along with financial implications. The OEWG can consider this paper and make a recommendation to the General Assembly for the establishment of the portal.

***