DRAFT WORKING PAPER ON THE ESTABLISHMENT OF A THREAT REPOSITORY WITHIN THE UNITED NATIONS

(as of 18 July 2023)

Introduction:

The Information and Communication Technology (ICT) landscape is ever changing and so is the threat landscape. The interconnected nature of technology in cyberspace makes it imperative for countries to collaborate and cooperate to address challenges around existing and potential threats in cyberspace.

In recognition that capacity, capability and threat landscape varies by region and State, and that a State has the primary responsibility for defining and outlining what constitutes a threat or cyber incident, at the multi-lateral level, a United Nations-run repository of cyber-related threats, will serve as a useful, non-attributionary, information and best practices sharing platform to leverage and assist small and developing countries in their preparedness, and identification of indicators of Compromise (IOC) . This will also allow for a deeper understanding of potential risks and their impact to enhance resilience of information and data security systems in the face of cyber threats given that these threats transcend international borders.

Such a repository of existing and potential threats for current and future system conditions will remain critical given the dynamism of types of threats within a system planning horizon. The repository will also allow a better appreciation of threats and timely, relevant, and actionable information for both national CERTS,, regional mechanisms and UN cyber security discussions.

Currently, there isn't a UN-run cyber threat repository. The UNIDIR Cyber Policy Portal does not have a repository feature. A few repositories and information sharing platforms exist, but these are regionally specific and/or focused, and exist outside the UN system[1].

Objective:

The purpose of Kenya's proposal is to establish a non-attribution UN-run cyber threat repository, that members can voluntarily and regularly update in the face of the constantly evolving and diversifying cyber threats. The cyber threat repository would be a centralized and accessible platform for cyber threat information sharing and facilitation of informed responses to cyber threat attacks, Indicators of Compromise and where possible best practices that articulate   how States have mitigated such threats.

Rationale /Justification:

The General Assembly resolution 75/240 recommended that the OEWG continue "*to study, with a view to promoting common understandings of existing and potential threats in the sphere of information security, interalia, data security, and possible cooperative measures to prevent and counter such threats*" (OP1)

As such, over the course of the OEWG sessions, beginning with the First Session to date, Member States continue to table what they consider as potential threats or malicious ICT activities. Often, the referenced threats have already occurred, and some addressed. However, there is no centralized platform to capture and archive these data. The increasing frequency and severity of cyber threats require a coordinated effort to address them effectively. The repository would therefore be a valuable resource for UN Member States in enhancing the security of their information and data systems. The repository will not only serve as a cyber threat repository, but as a knowledge portal as well.

The proposed repository would:

i. Enhance the efficiency and effectiveness of the response to such threats including potential risks before cyber incidents occur. This would enable countries to better prevent and mitigate the impact of such incidents.

[1] https://eurepoc.eu/; https://www.cfr.org/cyber-operations/; https://www.csirt.gob.cl/eng/noticias/strategic-role-of-misp-on-the-regional-exchange-information-model-used-by-csirtamericas/

Provide a platform for international cooperation, working alongside other national and regional mechanisms involved in addressing cyber threats.

ii. Allow for all subscribed member states to get timely information and be in a more informed position to undertake safeguards to secure their systems and infrastructure.

iii. Provide for foundational knowledge base for quick reference in Indicators of Compromise (IOC) and where possible remediations/mitigations that have been availed- a "how-to "portal.

iv. Enhance and uplift UN's visibility and the OEWG's role of actively championing its mandate of responsible state behaviors in cyberspace with real data.

Functionalities:

The repository would provide the following functionalities:

- A searchable database of common cyber threats and identified and noted Indicators of Compromise for the Threats.

- A platform for States to update information on new and emerging cyber threats and ability for subscribed members to get the same information on a real time basis

- Data visualization tools for effective analysis of the information, for example, the most recurrent threats including infrastructure type.

- Access controls and secure servers to ensure the confidentiality of the information shared by Member States

At the minimum, the repository shall reflect:

i. Identified Threat type e.g., malware or virus

ii. Threat characteristics/ (IOC) and how the threat manifests e.g., data encryption

iii. Delivery mode – e.g., email, download, URL,

iv. Exploitable vulnerabilities and targeted environments

v. Critical ICT infrastructure in various sectorse.g., banking, health systems

vi. Recommended deterrent, detection, and response measures

Operationalization, Management and Access:

The UN-run repository of common Cyber threats should have a dedicated team, who should be responsible for ensuring the integrity and security of the repository, as well as maintaining the database.

The proposed UN- run repository would be a web-based platform accessible to all Member States. Member States can agree on working principles of use and accessibility within the framework of the OEWG, and in complementarity with other agreed relevant initiatives within the OEWG. The repository shall be run in all UN languages.

The resources to operationalize this repository can be pulled through a collaborative approach.

The UN Office of Disarmament Affairs (UNODA) in collaboration with the UN Institute for Disarmament Research (UNIDIR) would serve as custodian of the repository through overseeing the platform including establishing the online mechanism for submission of information according to the modalities agreed by States; granting access to States as required; receiving information as submitted by States; and sending reminders to States to submit relevant information at a reasonable frequency.

As custodian, UNODA/UNIDIR will also ensure all information posted to the repository is fully in line with the agreed scope, objective, and principles of the repository including its non-attribution feature. Should any issues arise in this regard, UNODA/UNIDIR will liaise directly with the submitting State to resolve it in a judicious and appropriate manner.

There shall be two levels of access rights: read/view only and read/write rights.

Members states of the repository are encouraged to voluntarily share updates on threats as and when they occur and/or they become aware of them.

Also, any threats which the members of the repository feel have an impact on the assets of a State or organisation could be indicated as well in line with the agreed parameters. This would help in creating awareness, broaden knowledge and ensure proactiveness in the preparation on any for any possible threat.

Member States could agree on rules of access, steps of updating the repository and measures to be undertaken in instances where a member deliberately provides misleading information or violates the agreed upon rules of access including non-attribution.

END