Introduction:

The Information and Communication Technology (ICT) landscape is ever changing and so are the threat actors. 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.

A United Nations-run repository of common threats, vectors and actors will assist countries in their preparedness, identification of indicators of Compromise (IOC), a deeper understanding of potential risks and their impact and enhancing the resilience of information and data security systems in the face of cyber threats.

A repository of potential threats for current and future system conditions will remain critical given the dynamism of types of threats within a system planning horizon.

Objective:

The purpose of Kenya’s proposal is to establish a UN-run repository that members can voluntarily and regularly update in the face of new and emerging cyber threats. The repository would be a centralized and accessible platform for information sharing and facilitation of informed responses to cyber threat attacks, based on 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, inter alia, 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 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.

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

iii) Allow for all subscribed members to get timely information and be in a more informed position to undertake safeguards to secure their systems and infrastructure

Operationalisation:

The proposed UN-run repository of common threats, vectors and actors would be a web-based platform accessible to all subscribed Member States. Member States can agree on working principles of use and accessibility within the framework of 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) 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; sending reminders, at a reasonable frequency, to States to submit relevant information.
As custodian, UNODA will also ensure all information posted to the repository is fully in line with the agreed scope, objective, and principles of the repository. Should any issue arise in this regard, UNODA will liaise directly with the submitting State to resolve it in a judicious and appropriate manner.

**Functionalities:**

The repository would provide the following functionalities:

- A searchable database of common cyber threats, vectors, and actors, and identified and noted Indicators of Compromise for the Threats.
- A system for Member 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
- A system for Member States to request and provide assistance in addressing cyber threats
- Data visualization tools for effective analysis of the information for example, the most reported threats based on the region and 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:**

1. Threat type e.g., malware
2. Threat characteristics i.e., how the threat manifests e.g., data encryption
3. Vectors
4. Exploitable vulnerabilities
5. Target infrastructure e.g., banking, health systems
6. Recommended deterrent, detection, and response measures
7. Approximate date and time of discovery
Management and Access:

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

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

Members of the repository are encouraged to 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 reported as well. This would help members to be better prepared 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.