Misión Permanente de Costa Rica ante las Naciones Unidas
211 E. 43rd Street, Room 1002, New York, NY 10017. Tel: (212) 986-6373

III Session of the Open Ended Working Group on security of and in the use of information and communications technologies 2021-25.

Nueva York, 25 de Julio 2022

Delivered by José David Murillo.

Estimado señor Presidente,

Agradecemos el esfuerzo en presentar este segundo documento de cara a la III sesión del Grupo de Trabajo de Composición Abierta. Como Usted lo ha expresado, también tenemos la esperanza de alcanzar el consenso al final de esta sesión.

La versión 1 del documento es una excelente base para nuestras discusiones. Creemos que se reflejan las discusiones de este primer año de trabajo, así como las sugerencias de las delegaciones durante la sesión del 12 de julio pasado.
Permítame compartir algunas sugerencias y observaciones:

1. **Sobre la sección A, los párrafos introductorios**,
- En el párrafo 1, se podría valorar incorporar una referencia al *Derecho Internacional Humanitario*. Si bien estamos satisfechos con el modo cómo se ha abordado el tema en el capítulo sobre Derecho Internacional, Costa Rica prefiere que esta referencia se muestre también en los párrafos introductorios.
- En el párrafo 4, sobre los **esfuerzos regionales y subregionales**, entendemos el espíritu del texto, quizá se podría valorar utilizar la frase " *when applicable*" para clarificar que no todos los Estados tienen mecanismos regionales o que estos no desarrollan capacidades en temas de seguridad.
Costa Rica le otorga un alto valor a los esfuerzos *bottom up* que las capacidades regionales y subregionales le pueden imprimir a este grupo de trabajo, como lo expresa el parrafo 7c "*States proposed that there is value in regional and sub-regional organizations sharing relevant experiences at the OEWG as appropriate" o el parrafo 10.2* sobre points of contacts "*taking into account available best practices such as regional and sub-regional experiences where appropriate"* y creemos que la palabra complemetarios puede no ser acertada, quizá también se pueda usar la frase "*se complementan mutuamente*".

2. **En la sección B, Amenazas Existentes y Potenciales**:

En esta sección, Costa Rica desea destacar tres aspectos:

En primer lugar, para países en vías de desarrollo el secuestro de datos o *ransomware* se convierte en un problema de seguridad y hasta de emergencia nacional cuando el

blanco de los ataques son las mismas instituciones del Estado. Este ha sido el caso de Costa Rica desde abril 2022. **Creemos que la evidencia es clara para incluir el tema del *ransomware* como una amenaza real y vigente**.

En segundo lugar, las recomendaciones 2 y 3 podrían incluir intercambios entre expertos técnicos de diferentes regiones. Estos intercambios ofrecen una oportunidad dorada para que los Estados Miembros y los responsables políticos conozcan y comprendan mejor los aspectos técnicos de las cuestiones relacionadas con la respuesta a incidentes y la mitigación de los mismos, así como la protección de Infraestructuras Críticas (IC) y de la Infraestructura de Información Crítica (ICI).

En tercer lugar, la información sobre amenazas y la respuesta a incidentes es un área en la que las partes interesadas, como los CERT, las comunidades de CERT y las empresas de tecnología, cuentan un enorme valor agregado. Un recurso extremadamente valioso en este sentido es el Foro de Equipos de Seguridad y Respuesta a Incidentes (FIRST), ya que ofrece información sobre las mejores prácticas de funcionamiento y cooperación de los CERT.

3. **En la sección C, Reglas, Normas y Principios de Comportamiento Responsable de los Estados**, Costa Rica desea destacar cuatro aspectos.

En primer lugar, creemos en el valor de la Encuesta Nacional de Implementación y en el Reporte del Secretario General sobre el desarrollo en el campo de las Tecnologías de Información en el contexto de la Seguridad Internacional como instrumentos para fortalecer la confianza y ayudar a los Estados a identificar los retos en la construcción de capacidades, por lo que Costa Rica apoya y hace un llamado al grupo a trabajar sobre estas iniciativas.

En segundo lugar, Costa Rica recibe con satisfacción las recomendaciones para que los Estados sigan compartiendo documentos de trabajo y prácticas sobre la aplicación de las normas.

En tercer lugar, encontramos valor en el párrafo 8e sobre *las recomendaciones del Resumen del Presidente de 2021* a fin de continuar desarrollando la lista de propuestas que ahí se contemplan sobre este tema.

En cuarto lugar, para Costa Rica está claro que queda mucho trabajo por hacer para difundir lo que se ha acordado a nivel internacional a través de las estructuras nacionales de formulación de políticas y defensa. En este sentido, las organizaciones regionales, las estructuras como los centros de excelencia en cibercapacidad y los esfuerzos de capacitación para formar y educar a los responsables políticos y diplomáticos son fundamentales para solventar esta brecha, que es necesaria para la implementación real del marco normativo. Además de los intercambios de expertos, este Grupo podría

considerar el apoyo a un intercambio parlamentario, en el que los legisladores nacionales puedan comprender cómo se aplica el marco normativo y el derecho internacional a las políticas nacionales, y cómo las estrategias y políticas cibernéticas nacionales pueden integrar elementos de este marco. Un ejemplo de ello es la creación de procesos de divulgación de vulnerabilidades. El marco normativo de la ONU para el ciberespacio (norma 13j del GGE) fomenta la notificación responsable de las vulnerabilidades de las TICs. Para que esto tenga lugar a nivel internacional, los Estados debemos contar con procesos a nivel nacional. Existen mejores prácticas que podrían compartirse en lo que respecta al diseño de dichos procesos y políticas internas, incluso sobre cómo establecer una cooperación eficaz con el sector privado.

UNOFFICIAL COURTESY TRANSLATION

Dear Mr President,

We appreciate the effort in presenting this second document for the III session of the Open Ended Working Group. As you have reinforced, we also hope to reach consensus at the end of this session.

Version 1 of this document is an excellent basis for our discussions. We believe that the discussions of this first year of work are reflected, as well as the suggestions of the delegations during the session of July 12 last.

Let me share a few suggestions and observations:

1**. About section A, the introductory paragraphs,**

- In paragraph 1, it could be considered to include a reference to International Humanitarian Law. Although we are satisfied with the way in which the topic has been addressed in the chapter on International Law, Costa Rica prefers that this reference is also shown in the introductory paragraphs.

- In paragraph 4, on regional and subregional efforts, we understand the spirit of the text, perhaps it could be considered to use the phrase "when apply" to clarify that not all States have regional mechanisms or that they do not develop security issues.
Costa Rica gives a high value on the bottom-up efforts that regional and subregional capacities can provide to this working group, as expressed in paragraph 7c *"States proposed that there is value in regional and sub-regional organizations sharing relevant experiences at the OEWG as appropriate" or paragraph 10.2 about points of contacts taking into account available best practices such as regional and sub-regional experiences where appropriate"* and we believe that the word complementary may not be correct, perhaps the phrase "will complement one another" will be better understood.

2**. In section B, Existing and Potential Threats:**

In this section, Costa Rica wishes to highlight three aspects:

First, for developing countries, ransomware becomes a security problem and even a national emergency when the target of the attacks are the State institutions themselves. This has been the case in Costa Rica since April 2022. We believe that the evidence is solid enough to include the issue of ransomware as a real and current threat.

Second, recommendation 2 and 3 could be designed to include peer-to-peer exchanges among technical experts from different regions. These exchanges provide a golden opportunity for Member States and policymakers to be exposed to and more fully understand the technical aspects of issues related to incident response and mitigation and Critical Infrastructure (CI) and Critical Information Infrastructure (CII) protection.

Third, threat information and incident response is an area where stakeholders such as CERTs, CERT communities and tech companies have an outsized value added. The Forum of Incident Response and Security Teams (FIRST is an extremely valuable resource in this regard, offering insight on best practices for CERT operation and cooperation.

3. In section C, Rules, Norms and Principles of Responsible Behavior of States, Costa Rica wishes to highlight four aspects.

First, we believe in the value of the National Implementation Survey and the Report of the Secretary General on developments in the field of Information Technologies in the context of International Security as valuable instruments to strengthen trust and help States to identify the challenges in capacity building, for which Costa Rica supports and calls on the group to work on these initiatives.

Second, Costa Rica welcomes the recommendations for States to continue to share working papers and practices on implementation of norms.

Third, we find value in paragraph 8e on the recommendations of the 2021 Chair's Summary in order to further develop the list of proposals share on that document about this topic.

Fourth, it is clear for Costa Rica that there remains much work to be done in disseminating what has been agreed upon at the international level throughout national policymaking and defense structures. The roles of regional organizations, structures like cyber capacity centers of excellence and capacity building efforts to train and educate policymakers and diplomats are critical in closing this particular gap, which is necessary for real implementation of the normative framework. In addition to expert exchanges, the OEWG might consider supporting a parliamentary exchange, where national legislators can

understand how the normative framework and international law applies to national policies, and how national cyber strategies and policies can integrate elements of this framework. An example here is the creation of vulnerability disclosure processes. Responsible reporting of ICT vulnerabilities is encouraged in the UN normative framework for cyberspace (UN GGE norm 13j). In order for this to take place at the international level, governments must have processes in place at the national level. There are best practices which could be shared in regard to designing such processes and internal policies, including on how to establish effective cooperation with the private sector.