Intervención Paraguay
Sexta reunión del Grupo de Expertos encargado de Realizar un Estudio Exhaustivo sobre el Delito Cibernético
27 al 29 de julio

Gracias señor Presidente,

Paraguay celebra la realización de tan importante evento que posibilita reunirnos en el marco de temas de tanta trascendencia como lo son el ciberdelito y la ciberseguridad para compartir nuestros avances, desafíos comunes y necesidades en la materia.

En los últimos años, nuestro país ha avanzado significativamente en el ámbito que nos ocupa el día de hoy, en gran medida gracias a la cooperación internacional y al trabajo coordinado de las instituciones nacionales.

Entre los avances más resaltantes podemos mencionar la aprobación, en el 2017, del "*Plan Nacional de Ciberseguridad"* y la conformación de la Comisión Nacional de Ciberseguridad con representantes de distintas instituciones públicas. Estos logros se dieron gracias al apoyo de la Organización de los Estados Americanos.

El mismo año, nuestro país se adhirió a la Convención de Budapest sobre delincuencia cibernética y su Protocolo adicional, y actualmente, como Estado parte de esta Convención, somos beneficiarios del Programa GLAZY+ (Acción Global contra la Ciberdelincuencia extendida), llevado adelante por el Consejo de Europa conjuntamente con la Unión Europea, con el objeto de respaldar a los países miembros a fin de lograr la implementación y armonización efectiva de la Convención a la legislación positiva nacional.

En diciembre de 2019, hemos recibido a la Comitiva del Consejo de Europa a los efectos de realizar la Misión Inicial, compuesta por consultores expertos en el área de ciberdelincuencia, a fin de evaluar el estado en que se encuentra el país en el ámbito de lucha contra la ciberdelincuencia, con el objetivo de fijar los lineamientos a seguir a través de un plan de trabajo con los diversos actores intervinientes en el área de la delincuencia informática, plan que estamos implementando en la actualidad.

En octubre de 2018, fue creado el Ministerio de Tecnologías de la Información y Comunicaciones, dentro del cual se estableció la Ciberseguridad y Protección de la Información como un eje estratégico.

Asimismo, estamos evaluando adecuaciones en nuestra legislación nacional para así complementar las modificaciones realizadas al Código Penal en el 2011, en las que se amplió el catálogo de hechos punibles existentes, que hacen referencia a ciertos artículos que describen conductas ilícitas realizadas a través del uso de la tecnología, cuya esencia radica en su naturaleza informática, más conocida como delitos informáticos. En el mismo sentido, se está evaluando la modificación del código de procedimientos penales. También, actualmente se encuentra en el Parlamento un proyecto de ley *"De protección de datos personales.*

La arquitectura institucional nacional está compuesta principalmente, por una Unidad Especializada en Delitos Informáticos, del Ministerio Público, integrada por una Fiscalía Adjunta, una Fiscalía Delegada y tres unidades penales en la capital, así también cuenta con agentes fiscales especializados en ciberdelincuencia en las principales cabeceras departamentales, para intervenir en denuncias de hechos punibles de naturaleza informática. Por su parte, la Policía Nacional también cuenta con una División

especializada de lucha contra el Cibercrimen, que trabaja conjuntamente con el Ministerio Público.

Como parte de la estrategia nacional para responder a estas nuevas amenazas, el Ministerio de Defensa a través del Instituto de Altos Estudios Estratégicos, ha incorporado en su malla curricular el Programa de Especialización en Ciberdefensa y Ciberseguridad Estratégica en un proceso de innovación y adaptación a los nuevos tiempos.

En lo que respecta a la prevención, el Plan Nacional de Ciberseguridad establece en su quinto eje de acción"*la Capacidad de Investigación y Persecución de la Ciberdelincuencia"*. Asimismo, el MITIC, en su calidad de autoridad central en cuanto a Ciberseguridad, viene trabajando en un sistema de alertas tempranas de seguridad acerca de amenazas inminentes, estándares y lineamientos de seguridad específicos para sistemas de Gobierno, campañas de concienciación en ciberseguridad, capacitaciones a funcionarios de gobierno, a ciudadanos y al ecosistema en general, así como coordinaciones intersectoriales para contar con políticas y protocolos robustos en la materia, en un esfuerzo de minimizar el grado de exposición y vulnerabilidad de los sistemas, redes y procesos que involucran tecnologías, y así reducir la oportunidad para los cibercriminales.

Todas estas medidas para fortalecer las capacidades nacionales en esta área demuestran la firme voluntad del gobierno paraguayo para dar cumplimiento a los compromisos internacionales en la materia. No obstante, estos avances no hubieran sido posibles sin la cooperación internacional, en especial considerando nuestra condición de país en desarrollo sin litoral marítimo.

Finalmente, sostenemos que los Estados debemos seguir alentando la cooperación internacional, tanto a nivel bilateral como multilateral, en especial en el fortalecimiento de capacidades, intercambio de información (formal e informal), y buenas prácticas, basándonos en el principio de reciprocidad para así caminar al ritmo de los avances tecnológicos y luchar contra los grupos delictivos organizados, habida cuenta del carácter trasnacional de la ciberdelincuencia, en la seguridad de que ningún estado u organismo puede actuar solo para combatir estos flagelos.

Muchas gracias,