DOMPDF_ENABLE_REMOTE is set to FALSE
file:///var/www/html/portal_mincom_v2/sites/all/themes/mincom/logo.png

DOMPDF_ENABLE_REMOTE is set to FALSE
file:///var/www/html/portal_mincom_v2/sites/default/files/styles/noticias/public/vm_mincom_1.jpg

Fuente:
Tomado de Misiones Minrex

Intervención del viceministro del Ministerio de Comunicaciones de la República de Cuba, Ernesto Rodríguez Hernández, en la cuarta sesión sustantiva del GTCA sobre ciberseguridad 2021-2025. Debate sobre amenazas existentes y potenciales.

Señor Presidente:

Son diversas las amenazas que enfrentamos los Estados Miembros en la esfera de la seguridad de la información.

El creciente desarrollo de capacidades ciberofensivas y la inclusión en las estrategias de seguridad nacional de algunos Estados del uso de armas cibernéticas ofensivas y de la realización de operaciones ciberofensivas; así como la posibilidad de realizar ciberataques preventivos para disuadir adversarios, pueden convertir el ciberespacio en un nuevo escenario de conflicto. Ese peligro se acrecienta ante las doctrinas que consideran el uso de la fuerza como una respuesta legítima a un ataque cibernético.

El empleo encubierto e ilegal de los sistemas informáticos de otras naciones, por individuos, organizaciones y Estados, para realizar ataques informáticos en contra de terceros países, puede ser también un detonante de conflictos internacionales.

El uso indebido de las tecnologías de la información y las comunicaciones y de las plataformas de los medios de comunicación, incluidas las redes sociales y las transmisiones radiofónicas y electrónicas, como una herramienta para el intervencionismo mediante la promoción de discursos de odio, la incitación a la violencia, la subversión, la desestabilización, la difusión de noticias falsas y la tergiversación de la realidad contra cualquier Estado con fines políticos y como pretexto para la amenaza o el uso de la fuerza, representan también una amenaza para las naciones y contravienen los principios del Derecho Internacional.

Dichas acciones forman parte de la llamada guerra de cuarta generación, que trabaja sobre la base de la manipulación de las emociones, a partir del uso de información almacenada y procesada en violación de la protección a los derechos de datos personales, en lo que participan empresas que convierten en negocio ese modelo de actuación.

Reafirmamos el derecho y el deber que tienen los Estados de combatir, en el marco de sus prerrogativas constitucionales, la difusión de noticias falsas o distorsionadas que puedan interpretarse como una injerencia en los asuntos internos de otros Estados o como perjudiciales para la promoción de la paz, la cooperación y las relaciones amistosas entre Estados y naciones.

Cuba ha denunciado reiteradamente cómo se le limita el acceso a plataformas y servicios, se bloquean cuentas en las redes sociales, se obstaculizan inversiones para el desarrollo de las infraestructuras TIC; e hipócritamente se promueven alternativas para fomentar servicios fuera del control estatal con fines subversivos.

Todo ello tiene lugar en un contexto internacional de constantes amenazas a la paz y la seguridad por conflictos armados, guerras no convencionales, tentativas de cambios de régimen y frecuentes violaciones de la Carta de las Naciones Unidas y el Derecho Internacional, así como actos terroristas, incluido el terrorismo de Estado.

Para contrarrestar las amenazas anteriores, se requiere un compromiso global para el uso de las TIC con fines exclusivamente pacíficos, en beneficio de la cooperación y el desarrollo de los pueblos. Debe prohibirse el uso de las TIC como pretexto para el desencadenamiento de la guerra, la amenaza o el uso de la fuerza o como herramienta para el intervencionismo, la subversión, la desestabilización, la difusión de noticias falsas y la tergiversación con fines políticos; así como para campañas mediáticas de desinformación contra gobiernos soberanos. Debe establecerse una clara oposición a la militarización del ciberespacio.

Debe atenderse la colosal brecha tecnológica y los obstáculos impuestos a los países en desarrollo para invertir en la seguridad de sus infraestructuras TIC, que limitan sus capacidades para enfrentar las crecientes y complejas amenazas actuales y potenciales.

Se requiere adoptar, en el marco de las Naciones Unidas, un instrumento internacional jurídicamente vinculante, que complemente el derecho internacional aplicable, dé respuesta a los significativos vacíos legales en materia de ciberseguridad y permita atender de manera efectiva los crecientes retos y amenazas, a través de la cooperación internacional.

Teniendo en cuenta lo anterior, nos gustaría compartir algunas acciones que podrían contribuir a enfrentar las amenazas actuales y potenciales en el entorno de las TIC:

1. Incrementar la cooperación para enfrentar los incidentes cibernéticos, intercambiando información que no comprometa la privacidad de los Estados respecto a sus capacidades ni contravenga las legislaciones nacionales.
2. Implementar mecanismos de asistencia técnica para la creación de capacidades, incluidas aquellas para perfeccionar la protección de infraestructuras críticas, sobre la base del respeto a las legislaciones nacionales de los Estados.
3. Intercambiar buenas prácticas en el enfrentamiento a incidentes cibernéticos, sobre todo entre los Equipos de Respuesta ante Emergencias Informáticas (CERT, por sus siglas en inglés), para incrementar las capacidades operativas de los países ante un ciberataque.
4. Estandarizar, en la medida de lo posible, la nomenclatura de incidentes cibernéticos en la búsqueda de una terminología común, que facilite el intercambio de información en materia de respuesta a incidentes.
5. Establecer un mecanismo multilateral para determinar, de manera imparcial e inequívoca, el origen de los incidentes relacionados con el uso de las TIC.

Muchas gracias

https://bit.ly/3ZIGbzw [1]

Links
[1] https://bit.ly/3ZIGbzw