Image not found or type unknown

www.juventudrebelde.cu

Image not found or type unknown

Cuba es sede del Foro sobre el uso de las tecnologías con fines pacíficos. Autor: Internet Publicado: 09/07/2019 | 04:02 pm

¿En qué cibermundo queremos vivir?

El uso malicioso de las TIC amenaza con socavar la soberanía de los Estados e interferir en sus asuntos internos

Publicado: Martes 09 julio 2019 | 04:06:16 pm.

Publicado por: Yulia O.Tomilova

Los debates sobre la seguridad de la información internacional en el marco del Foro de La Habana permiten discutir los problemas en el ámbito de la seguridad de la información internacional más relevantes para la comunidad internacional y examinar conjuntamente los métodos para luchar eficazmente contra ellos.

Por desgracia, el número de desafíos relacionados con el uso ilegal de las TIC aumenta cada día. En el contexto, cuando el mundo depende cada vez más de las tecnologías digitales y corrientes de información, la fiabilidad de la información y la lucha contra las falsificaciones, cuya fabricación masiva puede tener consecuencias catastróficas, se convierte en la piedra angular.

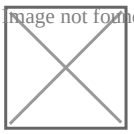
El uso malicioso de las TIC amenaza con socavar la soberanía de los Estados e interferir en sus asuntos internos. Desde hace tiempo muchos países consideran la protección contra ataques cibernéticos una prioridad de seguridad nacional de cada país desarrollado y a menudo comparan los medios de dicha protección con los sistemas de defensa antiaérea y de proyectiles antibalísticos.

Los grupos delictivos que posean las tecnologías y conocimientos en el ámbito de programación y seguridad de la información están pasando enérgicamente de los ataques simples a los activos financieros al chantaje y sabotaje a escala industrial. Los programas maliciosos se han convertido en una amenaza no solamente para el

funcionamiento de los ordenadores individuales, sino también para la existencia y el buen funcionamiento de sectores económicos enteros y de los organismos de seguridad nacional.

El mayor peligro radica en los incidentes cometidos en línea que puedan llevar a una guerra a gran escala fuera de línea. La doctrina de los llamados ataques cibernéticos preventivos, promovida por varios países, constituye una amenaza real para la paz y la seguridad internacionales. Se supone que el uso de la fuerza en respuesta a aún posibles ataques cibernéticos es un acto legítimo.

Por desgracia, algunos Estados ya están aplicando ese concepto en la práctica. Se hace sin resoluciones correspondientes del Consejo de Seguridad de las Naciones Unidas y en violación a la Carta de las Naciones Unidas. La parte acusada se ve privada de la oportunidad de defender sus derechos ante los tribunales. ¿Acaso eso es la aplicabilidad del derecho internacional en el espacio cibernético? Por el contrario, estas medidas contribuyen a la consolidación de la dictadura y el derecho de los poderosos en el entorno cibernético y socavan la confianza entre los Estados.



En Cuba, Foro sobre el uso de las tecnologías con fines pacíficos.

Carretera sin destino

Suscita preocupación la visión de muchos Estados de que el uso las TIC con fines militares es un acto legítimo. El llamado «derecho a la legítima defensa», interpretado unilateralmente se usa como un pretexto para las sanciones y el uso de fuerza. A nuestro juicio, este enfoque es inaceptable. Es importante excluir las situaciones en las que un Estado identifica libremente y independientemente una fuente potencial de ciberamenazas sin mostrar pruebas y da un golpe destructivo y punitivo.

Otro concepto «innovador», promovido enérgicamente por algunos Estados es la llamada «atribución colectiva» de la fuente de un ataque cibernético, bajo el principio de «vergüenza para el culpable» (name and shame). Esa teoría da a un grupo de países la oportunidad de acusar a un tercer Estado de cometer delitos en el espacio cibernético. Tradicionalmente se ha pasado por alto la credibilidad de la fuente de estos ataques y la presentación de estas pruebas. También consideramos que una promoción ulterior de este concepto pseudolegalista es una «carretera sin destino».

Hoy día, el progreso socioeconómico depende también de las TIC. Esas tecnologías marcan el ritmo del desarrollo de casi todos los programas de inversión modernos, sectores avanzados de la economía digital, inteligencia artificial, Internet de las Cosas, transporte no tripulado, ciudades inteligentes, telemedicina y otros productos derivados de la revolución científica y tecnológica. Sin embargo, hoy día, todos estos logros son extremamente vulnerables a las amenazas en el ámbito de la seguridad de la información internacional y son rehenes de ese problema político no resuelto.

Otro grave problema es el uso de las TIC con fines delictivos. Según las estimaciones de las Naciones Unidas, el daño oficial a la economía mundial por ciberdelincuencia en 2017 fue 1,5 billones de dólares de los EE.UU. Según el Foro Económico Mundial, esta cifra podría alcanzar los 8 billones de dólares de los EE.UU. en 2022 y superar el ingreso combinado del uso de Internet.

Rusia sigue pidiendo a la comunidad internacional que adopte medidas decisivas para combatir la delincuencia en el ámbito de uso de las TIC. Un paso significativo en esta dirección fue dado en diciembre de 2018, cuando la Asamblea General de las Naciones Unidas aprobó por mayoría de los votos la resolución rusa sobre la lucha contra la utilización de las tecnologías de la información y las comunicaciones con fines delictivos.

El objetivo principal de la iniciativa es iniciar un debate amplio y transparente sobre la lucha contra la delincuencia informática, buscar y formular respuestas a uno de los desafíos contemporáneos más pertinentes. Esperamos un diálogo más productivo posible sobre ese tema en las Naciones Unidas.

Creemos que los problemas indicados deben ser abordados bajo los auspicios de las Naciones Unidas con la participación activa de todos los miembros interesados de la comunidad internacional. Gracias a los esfuerzos de la gran mayoría de la comunidad internacional (120 países), tenemos una oportunidad real para llevar al siguiente nivel el proceso de negociaciones sobre la seguridad de la información internacional en las Naciones Unidas.

Se trata de la creación y el inicio de la labor por iniciativa de Rusia el 3?4 de junio en Nueva York de un Grupo de Trabajo de Composición Abierta de las Naciones Unidas sobre la Seguridad de la Información Internacional.

La diferencia fundamental de ese Grupo de Trabajo es que no es solamente una plataforma para el intercambio de opiniones entre expertos sino un órgano subsidiario de la Asamblea General encargado de la elaboración de decisiones concretas. Además, en el momento actual es el mecanismo más representativo en las Naciones Unidas dedicado a la seguridad de la información internacional. No son los expertos sino los Estados que pueden colaborar para resolver cuestiones de la seguridad global y nacional.

Nuestra causa común

El Grupo de Trabajo de Composición Abierta es nuestra causa común si queremos prevenir ciberanarquía en el mundo, si no queremos permitir agresión cibernética contra nuestros países o injerencia en los asuntos internos, comprometer estabilidad interna e inversiones.

El Grupo tiene una responsabilidad especial. Si muestra su incapacidad para llegar a un acuerdo sobre cuestiones básicas relacionadas con la seguridad de la información internacional, está pasivo o se limita a un enfoque estrictamente formal con respecto a su mandato, será una derrota no para países por separado sino para toda la comunidad internacional. Instamos a todos los Estados a realizar su derecho soberano y participar plenamente en las negociaciones en el Grupo de Trabajo de Composición Abierta, demostrando un espíritu constructivo y la intención de llegar a un compromiso.

El Grupo de Trabajo de Composición Abierta tiene pendiente una agenda amplia. Hay cuatro temas principales.

1. **Una prioridad absoluta en relación con la agenda internacional es la introducción de reglas/normas del comportamiento responsable de los Estados en el espacio ?ibernético.** El año pasado, la Asamblea General aprobó por primera vez la lista inicial de esas reglas/normas por mayoría abrumadora. Es un

logro sin parangón para la comunidad internacional. Nada semejante ha sido aprobado anteriormente. La lista tiene por objetivo prevenir conflictos en el espacio digital y consagrar en el mismo los principios de la no utilización de la fuerza, el respecto a la soberanía del Estado, la no injerencia en los asuntos internos de otros Estados, los derechos humanos y las libertades fundamentales, la prevención de la incorporación de funciones ocultas o programas espía en los productos comerciales de las TIC, productos conectados a Internet de las cosas por los que pagamos miles de millones.

En nuestra opinión, el paso siguiente será, de conformidad con el mandado del Grupo de Trabajo, seguir trabajando en la lista para que adquiera un carácter global, tanto como buscar formas de su aplicación. Todo eso permitirá universalizar esas reglas/normas.

2. **Medidas de fomento de la confianza en la esfera digital.** El Grupo de Trabajo podría, basándose en la experiencia regional, en particular, en el marco de la OSCE y el Foro Regional de la Seguridad de la ASEAN, considerar opciones para elaborar una lista global de tales medidas. Tal vez resulte útil considerar la armonización de las medidas de fomento de la confianza, acordados en regiones distintas, en el marco de las Naciones Unidas y adoptar criterios universales para esos fines que ayuden a elaborarlas en el futuro.
3. **El fututo de los debates sobre la seguridad de la información internacional en las Naciones Unidas.** En el momento actual está claro que ese tema se ha convertido en un elemento integrado de la agenda de la Organización. Ha llegado el momento de debatir las opciones para subirlo a un nivel nuevo, tal vez en forma de una estructura permanente bajo los auspicios de la ONU.
4. **Una tarea prioritaria es la facilitar la creación de capacidad digital de los países en desarrollo, salvar la brecha digital.** El ciberespacio necesita su propio arbitraje para prevenir y solucionar conflictos cibernéticos y no dar paso a acusaciones falseadas.

Para realizar las tareas mencionadas, se necesitarán esfuerzos negociadores intensos y rápidos. Esperamos que el Grupo de Trabajo demuestre un resultado visible y práctico de su trabajo. Le permitirá a la Asamblea General a no solamente empezar a tomar decisiones universales en esa esfera, sino también de hecho iniciar en las Naciones Unidas las negociaciones sostenidas sobre la seguridad de la información internacional.

(Yulia O.Tomilova, asistenta del representante especial del presidente de la federación de Rusia para la cooperación internacional en materia de la seguridad de la información Andréi V.Krutskij)

http://www.juventudrebelde.cu/ciencia-tecnica/2019-07-09/en-que-cibermundo-queremos-vivir