Tópico A: Avances en el campo de la información y las telecomunicaciones en el contexto de la seguridad internacional

La Asamblea General ocupa un lugar central como principal órgano deliberativo, de formulación de políticas y representativo de las Naciones Unidas. La Asamblea está integrada por los 193 Estados Miembros de las Naciones Unidas y proporciona un foro para el debate multilateral de toda la gama de cuestiones internacionales que abarca la Carta. Las decisiones sobre cuestiones consideradas importantes, como, por ejemplo, las recomendaciones relativas a la paz y la seguridad, la admisión de nuevos miembros y las cuestiones presupuestarias son tratadas por esta.

Debido a la enorme cantidad de temas, la Asamblea asigna la mayor parte de éstos a sus seis Comisiones Principales. Las Comisiones Principales consideran los puntos del programa que son transferidos a ellas por la Asamblea, y redactan recomendaciones y proyectos de resoluciones para presentarlas a las sesiones plenarias. Cada miembro tiene derecho a estar representado en cada una de las Comisiones Principales, que son las siguientes:

- Primera Comisión (Comisión de Desarme y Seguridad Internacional)
- Segunda Comisión (Comisión de Asuntos Económicos y Financieros)
- Tercera Comisión (Comisión de Asuntos Sociales, Humanitarios y Culturales)
- Cuarta Comisión (Comisión Política Especial y de Descolonización)
- Quinta Comisión (Comisión de Asuntos Administrativos y de Presupuesto)
- Sexta Comisión (Comisión Jurídica)

Algunas cuestiones se discuten sólo en sesión plenaria, y no en las Comisiones Principales. Todas las cuestiones se someten a votación en sesión plenaria, por lo común hacia el final del período de sesiones, luego de que las Comisiones hayan concluido el examen de esas cuestiones y presentado proyectos de resolución al pleno de la Asamblea General.

La Asamblea General reconoce que los avances científicos y tecnológicos pueden tener aplicaciones civiles y militares y que hay que mantener y fomentar el progreso científico y tecnológico en bien de las aplicaciones civiles; es notable como la ciencia y

tecnología ha avanzado a niveles que en un tiempo simplemente era un sueño, al poder ver cómo se pueden mantener comunicado a millones de personas de manera simultánea mediante las distintas herramientas utilizadas como los satélites de comunicaciones, redes computacionales, entre otros, que de cierta forma hace que la información llegue de manera rápida y efectiva.

Además, se ha discutido sobre los distintos métodos para la obtención de información, partiendo desde bases legales e ilegales, en donde en ocasiones, se produce un ataque a la confidencialidad y soberanía de naciones y organizaciones, infringiendo todos los aspectos en cuanto a seguridad nacional e internacional se refiere.

Uno de los principales hechos en donde se atenta contra la soberanía de las naciones, ha sido el espionaje, definiéndose como la práctica y al conjunto de técnicas asociadas a la obtención de información confidencial. Además de las tradicionales técnicas empleadas como la utilización de espías en la infiltración, sabotaje y encubrimiento de las misiones, actualmente se usan a gran escala los vehículos aéreos no tripulados o UAV (por sus siglas en inglés) en operaciones de reconocimiento y monitorio preciso de las operaciones; así como también la utilización de satélites espías, los cuales permiten realizar labores de inteligencia y comunicación con un espectro de visualización que puede cubrir toda la geografía mundial.

Si bien existen leyes que prohíben la visualización de ciertos sectores de los países sin consentimiento de las naciones involucradas, debido a su derecho de poseer un espacio aéreo reservado y confidencialidad de sus actividades, se tiene que hay más de 15 programas de satélites espías funcionando por naciones como Estados Unidos (Lacrosse/Onyx, Misty/Zirconio, Samos, etc.), Francia (Helios 1B, Helios 2A), Reino Unido (Circon), Alemania (SAR-Lupe 1-5), entre otras, los cuales le permite la obtención de información de manera inmediata y precisa sin previo consentimiento ni autorización.

Por otra parte, al visualizar como la evolución de las computadoras y las redes computacionales ha sido de manera sorprendente en los últimos años, desarrollando sistemas de información capaces de ayudar a controlar casi cualquier proceso de la vida productiva del hombre, logrando una dependencia única que en ciertos casos puede ser contraproducente, ya que si bien

pueden beneficiar al tener todo más controlado y organizado, también se puede dar el caso de abrir más brechas y facilidades para la obtención y manipulación de información de manera ilícita, considerándolo una preocupación para la seguridad nacional e internacional, porque así como se puede tener un balance de pago de una familia, se pueden tener los códigos de lanzamiento de cabezas nucleares e información crucial de inteligencia de los Gobiernos.

He aquí donde actúan los llamados crackers o sombreros negros, expertos en informática que usan su conocimiento con fines maliciosos, antimorales o incluso bélicos, como intrusión de redes, acceso ilegal a sistemas gubernamentales, robo de información, distribución de material ilegal o moralmente inaceptable, piratería, fabricación de virus y elementos de posible terrorismo como la comercialización de manuales para fabricar elementos explosivos caseros o la clásica tortura china.

Se estima que debido a los ataques informáticos, se pierden más de 55 billones de dólares al año, ocasionados por más de 100.000 ataques registrados. Se han detectado grandes intromisiones a entidades federales y gubernamentales que poseen información secreta y confidencial de las naciones, robando datos cruciales para luego ser vendidos o utilizados por otras entidades, tal como fue el caso de la entrada a los datos del Pentágono por parte de presuntos piratas rusos en 1999; así como también lo son los casos recientes, en donde se arrestaron a 4 expertos de la informática en Chile, involucrados en la penetración de los sistemas de seguridad de la Administración Nacional de Aeronáutica y Espacio (NASA por sus siglas en inglés) y el ataque del grupo de piratas informáticos Anonymous al Departamento de Justicia de los Estados Unidos Americanos. A su vez han existido diversos ataques a sitios web de los gobiernos de Israel, Venezuela, Turquía, entre otros.

De esta manera, se ha expresado gran preocupación sobre los riesgos inmediatos del uso de los diversos sistemas de información y comunicación, en donde se perjudique de manera directa o indirecta los principios de equidad y respeto mutuo de las naciones, la no-interferencia en los asuntos internos de la soberanía de los estados, la solución pacífica de disputas, el no-uso de la fuerza y respeto por los derechos humanos, y en la paz y estabilidad de la seguridad nacional e

internacional de todas las naciones implicadas.

¿Qué medidas serían convenientes para mantener un monitoreo constante de las actividades informáticas y de telecomunicación, así como las posibles consecuencias que puedan ocurrir en caso de usos no debidos?

¿Cómo se podrían llevar a cabo las diferentes medidas coercitivas necesarias para reprimir los presentes y futuros ataques que se puedan suscitar, así como también las posibles disposiciones para prevenirlos?

Bibliografía

Czinkota, M. R., & Ronkainen, I. A. (2007). *Negocios Internacionales* . Madrid: Cengage Learning Editores.

Instituto del Tercer Mundo. (2005). *Guía del Mundo: El mundo visto desde el sur.* Montevideo: Fundación Santa María.

National Commission on Terrorist Attacks. (2005). *11-S el informe:extracto del informe final de los atentados terroristas contra Estados Unidos.* España: Paidós.

Nelson, J. (2002). *El negocio de la paz: el sector privado como socio en la prevención y resolución del conflicto.* Colombia: Editorial Norma