GUÍA ACADÉMICA ASAMBLEA GENERAL III

Presentación:

Bienvenidos delegados al MONUR 2023, durante los próximos meses presenciarán una de las experiencias más hermosas que tiene la vida académica. Algunos ya habrán experimentado modelos anteriores y para otros, está será su primera vez. Siendo esta la décima edición del modelo, desde el equipo de presidencia les aseguramos que este año será tan o más grande y espectacular qué años anteriores y que van a disfrutarlo al máximo, esperamos conocerlos pronto y aprender juntos.

Equipo de presidencia:

El equipo de presidencia de esta comisión este año estará conformado por los siguientes integrantes:

- Andreani Theo Valentino, estudiante de último año del Instituto Juvenilia. Participó como delegado en MINU en las ediciones de 2018 y 2019. Durante su participación en MINU fue ganador de numerosos premios y menciones, Modelo que ha presidido en su edición 2022.
- Teper Agustina, estudiante avanzada y tesista de la Licenciatura en Ciencia Política de la UNMDP. Participó como delegada en varios modelos siendo los principales el MUNU como delegada de Brasil (AG) y como delegada de la República Popular China en el MONUBA, ganando dicho modelo y obteniendo el premio a mejor delegación.

Sobre la Comisión:

La Asamblea General III asignará el tratamiento de los temas específicos del órgano a representar. Los/as participantes deben asumir el papel de representantes de países y seguir una serie de reglamentos y normas de procedimientos similares a las que utilizan los delegados en las reuniones de los diferentes órganos de Naciones Unidas. Como delegados respectivos de cada nación tienen el deber de llevar a cabo un proceso de preparación e investigación de los tópicos, y tener una idea clara de la posición de los países en relación con los temas en debate.

La Asamblea General es una de los mayores órganos deliberativos de las Naciones Unidas, la cual está integrada por todos los miembros de las Naciones Unidas. En específico, este órgano va a estar integrado por todos los miembros de las Naciones Unidas, cada uno con un voto (exceptuando a aquellos los estados observadores no miembros como lo son el Estado de Palestina y el Vaticano o Santa Sede). En este órgano deliberativo de la ONU se podrá discutir acerca de cualquier asunto o cuestión, dentro de los límites de la Carta de las Naciones Unidas, o que se refieran a los poderes y funciones de los otros órganos creados por la Carta de las Naciones Unidas.

La Asamblea General podrá considerar los principios generales de la cooperación en el mantenimiento de la paz y la seguridad internacionales, incluso los principios que rigen el desarme y la regulación de los armamentos, y podrá también hacer recomendaciones respecto de tales principios a los Miembros o al Consejo de Seguridad o a éste y a aquéllos. Además podrá discutir toda cuestión relativa al mantenimiento de la paz y la seguridad internacionales que presente a su consideración cualquier Miembro de las Naciones Unidas o el Consejo de Seguridad.

La Asamblea General promoverá estudios y hará recomendaciones para los fines siguientes; fomentar la cooperación internacional en el campo político e impulsar el desarrollo progresivo del derecho internacional y su codificación;

Continuando con lo anterior, la Asamblea General es el órgano más amplio de las Naciones Unidas, por ende existen varias comisiones que se encargaran de tópicos específicos, en este caso representaremos a la Asamblea General III con el tópico que mencionaremos a continuación. Consideren pertinente a la hora de configurar el proceso de investigación y preparación -incluyendo los debates, discursos, anteproyectos y resoluciones- tomar en cuenta los tópicos correspondientes. Otras cuestiones a tratar que pueden surgir en el desempeño del Modelo serán en perspectiva secundaria. En efecto el tópico que preparamos para este año y que les introduciremos en las siguientes páginas, es el siguiente:

"Ciberdelito y globalización. Ataque a base de datos y servidores nacionales. Rol de la comunidad internacional en la preservación de las libertades individuales. Lucha contra la utilización de las tecnologías con fines delictivos."

Reseña Histórica:

La cuestión del ciberdelito en el contexto de la globalización ha emergido como un desafío crucial en el siglo XXI. El advenimiento de la era digital ha transformado radicalmente nuestra forma de vida y nuestras interacciones. La globalización, caracterizada por la interconexión y la interdependencia entre naciones, ha brindado un contexto propicio para el surgimiento del ciberdelito. Los delincuentes han aprovechado la falta de fronteras físicas en el ciberespacio para llevar a cabo ataques a bases de datos y servidores nacionales, comprometiendo la seguridad de gobiernos, empresas y ciudadanos.

Los ataques a bases de datos y servidores nacionales han adquirido una magnitud alarmante en los últimos años. Los ciberdelincuentes utilizan diversas técnicas, como el malware, el phishing y la explotación de vulnerabilidades, para infiltrarse en sistemas informáticos y acceder a información confidencial. Estos ataques pueden tener graves consecuencias, incluyendo el robo de datos sensibles, el sabotaje de infraestructuras críticas y la violación de la privacidad de las personas.

Ante la creciente amenaza del ciberdelito, la comunidad internacional ha reconocido la importancia de preservar las libertades individuales en el entorno digital. Se han establecido normas y acuerdos internacionales para garantizar la protección de los derechos

humanos en el ciberespacio. Organizaciones como las Naciones Unidas, la Unión Europea y la Organización de los Estados Americanos han desempeñado un papel crucial en la promoción de la cooperación internacional y la adopción de medidas para salvaguardar las libertades individuales en línea. Un claro ejemplo de esta problemática se ha dado en el 2017 cuando ocurrió el ataque masivo de ransomware WannaCry, que afectó a organizaciones en todo el mundo, incluyendo a instituciones gubernamentales y hospitales. Este incidente, junto a muchos otros, ha puesto de manifiesto la necesidad de una respuesta coordinada a nivel internacional para hacer frente a los ciberataques de gran escala.

Hay una creciente preocupación sobre el uso indebido de la tecnología de la información y las comunicaciones (TIC) por terroristas, en particular Internet y las nuevas tecnologías digitales, con el objetivo de cometer actos terroristas y realizar actividades de incitación, reclutamiento, financiación o planificación para actos de terrorismo. Los Estados Miembros han recalcado la importancia de que las múltiples partes interesadas cooperen para hacer frente a esta amenaza, en particular los Estados Miembros, las organizaciones internacionales, regionales y subregionales, el sector privado y la sociedad civil. En la resolución 2341 (2017), el Consejo de Seguridad exhorta a los Estados Miembros a "establecer o reforzar las alianzas nacionales, regionales e internacionales con las partes interesadas, tanto públicas como privadas, según proceda, para intercambiar información y experiencias a fin de prevenir, proteger, mitigar e investigar los daños causados por atentados terroristas contra instalaciones de infraestructura vital, así como para responder a ellos y recuperarse de ellos, en particular mediante actividades conjuntas de capacitación, y la utilización o el establecimiento de redes de alerta de emergencia o de comunicación pertinentes".La lucha contra la utilización de las tecnologías con fines delictivos requiere un enfoque integral y multidimensional. Los estados y las organizaciones internacionales han implementado estrategias para prevenir, detectar y responder a los ciberataques. Esto implica fortalecer la seguridad cibernética, mejorar la capacidad de respuesta a incidentes, promover la educación y concienciación sobre la ciberseguridad, así como fomentar la cooperación entre los actores estatales y no estatales.

Marco Legal:

La regulación en ciberseguridad y ciberdelito es de índole compleja, ya que es difícil dilucidar las relaciones entre lo público y privado, en consideración con las libertades individuales.
En el contexto de ciberseguridad y ciberdelito, es fundamental comprender el marco legal que respalda las fronteras de lo posible en estos ámbitos tan recientes pero complejos respectivamente. A continuación, se presentan algunos instrumentos legales y resoluciones de relevancia en materia de protocolos, convenios, convenciones y directrices que les ayudarán a abordar y entender el tópico en cuestión:

Declaración Universal de Derechos Humanos

Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional (Convención de Palermo)

Convenio sobre Ciberdelincuencia de Budapest (Convenio de Budapest)

Declaración de Principios sobre la Gobernanza del Internet

Convención de las Naciones Unidas sobre el Uso de las Comunicaciones Electrónicas en los Contratos Internacionales

Directrices de la OCDE para la Protección de la Privacidad y la Seguridad de la Información

Directiva de la Unión Europea sobre Seguridad de las Redes y la Información (Directiva NIS)

Convenio del Consejo de Europa sobre Cibercriminalidad

Declaración sobre el Acceso Gubernamental a Datos Personales en Posesión de Entidades del Sector Privado (OCDE)

Recuerden, que más allá de este marco legal general, ustedes deberían realizar una búsqueda en materia legal del tópico para estar informados sobre su país. En este marco que hemos proporcionado, no todo abarca y afecta la totalidad de países que se encuentran en la presente Asamblea General, es por esto que enfatizamos las búsquedas adicionales.

Convenios y protocolos internacionales de las Naciones Unidas

● Convenio de 1963 sobre las infracciones y ciertos otros actos cometidos a bordo de las aeronaves, y su Protocolo complementario de 2014;
● Convenio para la represión del apoderamiento ilícito de aeronaves de 1970, y su Protocolo complementario de 2010;
● Convenio para la represión de actos ilícitos contra la seguridad de la aviación civil de 1971;
● Convención de 1973 sobre la prevención y el castigo de los delitos contra las personas internacionalmente protegidas;
● Convención de 1980 sobre la protección física de los materiales nucleares;
● Convenio de 1988 para la represión de actos ilícitos contra la seguridad de la navegación marítima;
● Protocolo de 1988 para la represión de actos ilícitos contra la seguridad de las plataformas fijas emplazadas en la plataforma continental;
● Protocolo de 1988 para la represión de actos ilícitos de violencia en los aeropuertos que prestan servicio a la aviación civil internacional, complementario del Convenio para la represión de actos ilícitos contra la seguridad de la aviación civil;

● Convenio Internacional para la Represión de los Atentados Terroristas con Bombas de 1997;
● Enmiendas de 2005 a la Convención sobre la protección física de los materiales nucleares;
● Convenio Internacional para la Represión de los Actos de Terrorismo Nuclear de 2005;
● Protocolo de 2005 para la represión de actos ilícitos contra la seguridad de las plataformas fijas emplazadas en la plataforma continental;
● Protocolo de 2005 del Convenio para la represión de actos ilícitos contra la seguridad de la navegación marítima;
● Convenio para la Represión de Actos Ilícitos Relacionados con la Aviación Civil Internacional de 2010.

Los países correspondientes a los convenios y protocolos mencionados están obligados a configurar sus marcos jurídicos nacionales de una manera transversal. No obstante, los actos ligados al ciberterrorismo concierne a la actuación de cada país por parte de lo que se considere pertinente actuar.

Objetivos de debate:

En el marco de esta Asamblea General, el objetivo principal del debate es abordar la problemática del ciberdelito y la globalización, enfocándonos específicamente en los ataques a bases de datos y servidores nacionales, así como estos llevan a la apropiación de datos personales. El propósito de estas discusiones es promover un análisis integral de la situación actual, sus consecuencias y riesgos, centrándonos especialmente en la protección de los datos personales y las libertades individuales en línea, siendo esto lo vulnerado en materia de una deficiente ciberseguridad.

Para lograr un debate fructífero, se fomentará un ambiente de respeto y apertura, donde todas las delegaciones tengan la oportunidad de expresar sus puntos de vista.

Asimismo, se alienta a las delegaciones a considerar la importancia de la cooperación internacional en la prevención y mitigación de los ataques cibernéticos. Se busca establecer un marco legal sólido que promueva la colaboración entre países, facilitando el seguro intercambio de información y la coordinación de acciones conjuntas para hacer frente a las amenazas cibernéticas (Que afecten tanto al sector público como al privado).

En el contexto del debate, y el anteproyecto de resolución, se espera que las delegaciones propongan medidas concretas para proteger los datos personales y garantizar la privacidad en línea.

El objetivo final del debate que culminará en la aprobación del proyecto de resolución, es llegar a resoluciones consensuadas que reflejen el compromiso de la comunidad internacional y de los países presentes en la asamblea en relación al tópico en cuestión. Se insta a las delegaciones a trabajar juntas para forjar un enfoque integral y equilibrado que aborde la seguridad cibernética sin comprometer los derechos fundamentales de las personas en línea.