Legal

Sexta Comisión de Asuntes Legales y Jurídicos

MSMUN 2025

Mesa

Maximiliano Echeverri

Luciana Araque

Lenguaje Oficial

Español

Tema A

Revisión y Desarrollo de Tratados Internacionales Clave sobre Desarme y No Proliferación de Armas

Tema B

Las políticas del ciberespacio y los crímenes cibernéticos

1. Carta de Bienvenida

Queridos delegados,

Es un placer para nosotros darles la bienvenida al modelo de las naciones unidas del colegio Marymount MSMUN' 25 y especialmente a La Sexta Comisión para Asuntos Jurídicos y Legales. Somos Luciana Araque y Maximiliano Echeverri, y nos sentimos completamente honrados de tener el placer de dirigir y trabajar junto a ustedes en esta oportunidad de aprender sobre ti mismo, sobre los demás y sobre nuestra realidad. Como sus presidentes deseamos que durante estos tres días, el comité pueda desarrollarse de la mejor manera, que puedan expandir todos sus horizontes, aprendan nuevas cosas, que vean diferentes puntos de vista y que luchen por el mundo que todos anhelamos, este es el momento para alzar tu propia voz.

Lo más sorprendente sobre este modelo es que nos ha mostrado lo que somos capaces de lograr y hasta dónde somos capaces de llegar con trabajo duro, dedicación y perseverancia. Sabemos que puede dar miedo participar en este tipo de eventos, pero ya han demostrado un valor extraordinario al decidir participar. Estamos seguros que cada delegado tiene todas las capacidades y que se sorprenderán de lo mucho podrán lograr. Finalmente, los invitamos a que se adentren en el comité con la máxima determinación. Nuestras expectativas son muy altas, pero sabemos que las podrán superar. Además, les aseguramos que ambos trabajaremos incansablemente para hacer de MSMUN una experiencia inolvidable para cada uno de ustedes

Atentamente,

Presidente Araque: 305 3311880 Presidente Echeverri: 310 3722027

2. Introducción al comité

2.1 Historia del comité

Tras la Segunda Guerra Mundial, el mundo se encontraba en ruinas. La comunidad internacional vio la necesidad de establecer una entidad que permitiera la regulación de diferentes dinámicas de orden global y comprendiera tanto dinámicas de conflictos internacionales como las mismísimas leyes que rigen el comportamiento. Es por esto que, del 26 de abril al 25 de junio de 1945, se dio la Conferencia de las Naciones Unidas sobre Organización Internacional en San Francisco; dentro de esta se redactó y firmó la carta magna con la cual oficialmente se creó la Organización de las Naciones Unidas.Es necesario entender que la Asamblea general está estructurada por seis comités principales; a saber:

Comisión de Desarme y de Seguridad Internacional;

Comisión de Asuntos Económicos y Financieros;

Comisión de Asuntos Sociales, Humanitarios y Culturales;

Comisión de Política Especial y de Descolonización;

Comisión de Asuntos Administrativos y de Presupuesto;

Comisión Jurídica o legal.

El sexto comité de la asamblea general ha sostenido setenta y siete sesiones ordinarias y treinta y dos periodos extraordinarios; igualmente, se han dado once periodos de emergencia que se han otorgado por solicitud del consejo de seguridad.

2.2. Objetivos del comité

El sexto comité de la asamblea general de las Naciones Unidas, también conocido como el comité jurídico o legal, es uno de los principales comités de la asamblea general cuyo propósito es lidiar con temas de índole legal y poner a consideración cualquier asunto referente a las leyes internacionales que conciernen a los miembros de la organización. Esta comisión se dedica enteramente a la examinación de cuestiones jurídicas de la asamblea o a la revisión de asuntos que sean comunicados por los países miembros. Cabe recalcar que todos los países miembros de la ONU tienen derecho a reconocimiento dentro de la sexta comisión. Además, el propósito de este comité es apoyar la misión de paz y seguridad internacional por medio de las leyes que rigen las relaciones internacionales

3. TEMA A: Revisión y Desarrollo de Tratados Internacionales Clave sobre Desarme y No Proliferación de Armas

3.1 Introducción al tema

Desde su fundación, la Organización de las Naciones Unidas ha enfocado su esfuerzo en mantener la paz y la seguridad a nivel mundial en el desarme y la restricción de armas.
La reducción y eventual eliminación de las armas, que constituyen algunas de las amenazas más graves a las que se enfrenta la especie humana, ha sido priorizada por la ONU.
A pesar de que estos objetivos han permanecido constantes a lo largo del tiempo, el ámbito de las discusiones y conversaciones ha cambiado a medida que cambian las circunstancias políticas y la situación global.
La comunidad internacional se enfrenta a la proliferación de armas que amenazan a las sociedades y afectan negativamente a las personas, especialmente a los más vulnerables.
Además, se está volviendo más consciente de que los diversos tipos de armas tienen un impacto desigual en individuos de diversos géneros y edades.

3.2 Origen

Desde el final de la Segunda Guerra Mundial, el desarme y la no proliferación de armas han sido temas importantes en la diplomacia internacional. La comunidad internacional ha acordado una serie de tratados y convenciones para limitar el desarrollo y uso de armas nucleares y otras armas debido a la creciente amenaza que representan.
En 1899 y 1907, se llevaron a cabo las Conferencias de La Haya, que establecieron un marco para las negociaciones sobre limitaciones en armamentos y promovieron la paz a través del diálogo multilateral. No obstante, fue durante la Guerra Fría cuando se intensificó la lucha

por controlar las armas nucleares. En este período, hubo intensas tensiones entre las potencias nucleares, lo que condujo a la firma de importantes acuerdos, como el Tratado sobre la No Proliferación de las Armas Nucleares (TNP) en 1968. El objetivo de este acuerdo es evitar la proliferación y promover el desarme entre los países que las poseen.

En los últimos años, ha surgido una iniciativa de ayuda humanitaria que convoca a Estados y organizaciones no gubernamentales para buscar soluciones al actual estado de desarme. El resultado final de esta iniciativa fue la aprobación del Tratado sobre la Prohibición de las Armas Nucleares (TPAN), el primer tratado internacional que prohíbe completamente el uso de armas nucleares. El TPAN se fundamenta en valores humanitarios y tiene como objetivo deslegitimar estas armas en todo el mundo.

Los esfuerzos por lograr un desarme efectivo siguen enfrentando importantes desafíos, a pesar del marco legal existente. Uno de los principales desafíos es la falta de participación de algunos Estados armados en negociaciones importantes como el TPAN, lo que ha sido criticado porque reduce la efectividad del tratado. Además, los cambios geopolíticos actuales han complicado aún más los esfuerzos por avanzar hacia un desarme efectivo, haciendo necesario un cambio en el paradigma de seguridad internacional.

3.3 Situación actual

La situación actual del desarme y la no proliferación de armas está marcada por una serie de importantes desafíos que requieren una atención inmediata en el marco de la diplomacia internacional. Estos son los elementos más relevantes:

a. Tensiones globales

Una serie de conflictos y rivalidades han intensificado las tensiones entre naciones con capacidades bélicas significativas, poniendo en duda principios fundamentales del *ius ad bellum*, es decir, el derecho a recurrir a la guerra. Por ejemplo, el conflicto en Ucrania ha deteriorado gravemente las relaciones entre Estados Unidos y Rusia, quienes han reforzado sus fuerzas militares y revitalizado discursos belicistas. Esta situación incrementa el riesgo de enfrentamientos que violarían el *ius in bello* o las normas del derecho de la guerra, dado que cualquier conflicto moderno tendría graves consecuencias para la población civil.

El Tratado de No Proliferación Nuclear (*TNP*), aunque busca prevenir la proliferación y fomentar el desarme, ha sido limitado en su efectividad, pues muchos estados nucleares no han mostrado voluntad de cumplir con las promesas de desarme. Esta falta de progreso ha alimentado una percepción entre los países no nucleares de que el desarme es una meta lejana y prácticamente inalcanzable dentro de la agenda internacional, desalentando la cooperación en foros multilaterales.

b. Problemas Legales y Normativos relacionados con el Desarme Nuclear

Los obstáculos legales relacionados con el desarme son complejos y tienen un impacto en la ejecución de los acuerdos previos. La falta de mecanismos efectivos para verificar el cumplimiento es uno de los principales obstáculos. Los programas son difíciles de supervisar

internacionalmente debido a su naturaleza confidencial. Aunque el Organismo Internacional de Energía Atómica (OIEA) lleva a cabo inspecciones, su eficacia depende del acceso a las instalaciones y de la colaboración de los estados.

La creación de zonas libres de armas nucleares (ZLAN) es una estrategia beneficiosa, sin embargo, su ejecución requiere un compromiso político por parte de todos los estados involucrados. Aunque se reconoce el derecho a establecer estas zonas en el Tratado sobre la No Proliferación de las Armas Nucleares (TNP), la falta de voluntad política de algunos estados poseedores pone en peligro su efectividad.

Además, la falta de claridad en la elaboración de ciertos acuerdos puede resultar en interpretaciones divergentes sobre las responsabilidades de los países, dificultando la colaboración internacional. Es común que los países den más importancia a su *imperium* —su soberanía nacional— que a sus obligaciones internacionales, lo que puede obstaculizar la firma de nuevos acuerdos.

c. Proyectos de ayuda humanitaria

La Iniciativa Humanitaria es un esfuerzo internacional que busca cambiar la narrativa sobre las armas al centrarse en sus consecuencias humanitarias devastadoras en respuesta a la parálisis en el desarme. En 2012, un grupo de dieciséis países no nucleares, incluyendo Suiza y Noruega, lideró esta iniciativa junto a organizaciones de la sociedad civil para fomentar un enfoque alternativo al desarme nuclear.

La Iniciativa Humanitaria se basa en dos premisas fundamentales: que "las armas de destrucción masiva no deben ser empleadas en ninguna circunstancia" y que "la única forma de garantizar la eliminación del riesgo de una detonación altamente mortal es mediante su eliminación total". El discurso sobre el desarme se ha reformulado a partir de estas premisas,

desplazando el enfoque tradicional que se enfocaba en la estabilidad estratégica hacia uno que se enfocaba en las consecuencias humanitarias del uso de armamento.

Desde el comienzo, se han llevado a cabo numerosas reuniones humanitarias con el fin de debatir los efectos devastadores de la utilización de armas nucleares. En marzo de 2013, se llevó a cabo la primera conferencia en Oslo, que reunió a representantes de 120 países. Estos debates han aumentado la conciencia sobre los peligros de las armas nucleares y han cambiado significativamente la percepción global de estas armas. Esta iniciativa ha sido impulsada principalmente por la campaña internacional ICAN, que ha contribuido a aumentar la presión internacional para prohibir las armas nucleares. En 2017, ICAN recibió el Premio Nobel de la Paz en reconocimiento a sus iniciativas.

d. desarrollo sostenible

1. La relación entre el desarme y el progreso

Es cada vez más evidente que el desarme armamental y el desarrollo sostenible están estrechamente relacionados. El desarme puede ayudar no solo a la paz mundial sino también a la protección del clima. Se calcula que las fuerzas armadas son responsables de al menos el 5% de las emisiones globales de carbono, lo que demuestra la urgencia de incorporar el desarme en las conversaciones sobre desarrollo sostenible y cambio climático. La producción y las operaciones militares tienen un impacto ambiental significativo, lo que contribuye al cambio climático. Se ha registrado que las fuerzas armadas de Estados Unidos emiten más emisiones de carbono que una gran cantidad de países desarrollados. Esto plantea una pregunta importante: ¿cómo se pueden reorientar los fondos destinados a la inversión militar hacia iniciativas que aborden problemas ambientales críticos?

2. Recursos financieros

La redistribución de los recursos actualmente destinados al gasto militar hacia iniciativas climáticas podría liberar recursos significativos para abordar los efectos del cambio climático, especialmente en países en desarrollo. Se ha sugerido que sólo el diez por ciento del gasto militar global podría cubrir los gastos necesarios para hacer frente al cambio climático. Esto incluye la inversión en energías renovables, la creación de infraestructura resistente y la implementación de programas sociales para reducir los efectos ambientales.

La iniciativa "Traslade el dinero de las armas nucleares" tiene como objetivo disminuir los fondos destinados a la defensa en relación con las armas nucleares y dirigir dichos recursos hacia proyectos ambientalmente sostenibles. Para aumentar la conciencia sobre cómo el desarme puede contribuir a objetivos más amplios relacionados con el desarrollo sostenible, esta campaña combina la educación pública con la acción política.

d. Instrumentos internacionales

1. Los principales tratados

La importancia del Tratado sobre la No Proliferación de las Armas Nucleares (TNP) sigue siendo crucial para evitar la proliferación nuclear y promover el desarme. Ha sido ratificado por 190 países desde su inicio en 1970, incluyendo cinco potencias nucleares reconocidas: Estados Unidos, Rusia, China, Francia y el Reino Unido. No obstante, la falta de compromiso de algunos estados nucleares para avanzar hacia el desarme total pone en peligro su eficacia. Los problemas estructurales que enfrenta el TNP incluyen las notables disparidades entre los estados poseedores y no poseedores en cuanto a las expectativas de desarme. Los primeros sostienen que es necesario proteger sus arsenales ante posibles amenazas externas, mientras

que los segundos exigen acciones concretas para lograr un mundo sin armas nucleares como condición de su colaboración.

2. Conferencias Internacionales

La Conferencia sobre el Desarme (CD) sigue siendo el foro principal de las conversaciones multilaterales sobre el desarme nuclear. A pesar de haber alcanzado algunos logros significativos en el pasado, como la Convención sobre la Prohibición del Desarrollo y Producción de Armas Químicas, actualmente enfrenta desafíos importantes debido a la falta de acuerdo entre sus miembros.

Es difícil llegar a un acuerdo sobre temas importantes como la prohibición total del uso de armas nucleares o el desarrollo de nuevas tecnologías militares debido a las divisiones geopolíticas. Esto ha llevado a un estancamiento prolongado, donde muchos estados sienten que sus preocupaciones no se escuchan ni se abordan adecuadamente.

En conclusión la situación actual del desarme es complicada y está relacionada con una variedad de factores geopolíticos, humanitarios y normativos. Las tensiones entre las potencias continúan obstaculizando los esfuerzos hacia un mundo pacifico. Por otro lado, las iniciativas humanitarias ofrecen caminos alternativos para abordar estos desafíos desde una perspectiva centrada en las consecuencias sociales del uso de armas. Teniendo diferentes perspectivas encontradas, los países deben encontrar un punto medio en el marco legal internacional que cree un compromiso colectivo para poder avanzar hacia un mundo libre de violencia y garantizar así una paz duradera para futuras generaciones.

3.4 Resoluciones previas

- **Resolución 1540 (2004):** Adoptada por el Consejo de Seguridad de las Naciones Unidas el 28 de abril de 2004, esta resolución establece obligaciones para los Estados con el fin de prevenir la proliferación de armas de destrucción masiva (ADM) por actores no estatales. Reconoce la proliferación de armas químicas, biológicas y nucleares como una amenaza a la paz y la seguridad internacionales, y complementa tratados existentes como el Tratado sobre la No Proliferación de Armas Nucleares (TNP) y la Convención sobre Armas Químicas.
- **Tratado sobre la No Proliferación de las Armas Nucleares (TNP):** Este tratado, abierto a la firma en 1968 y en vigor desde 1970, es fundamental para los esfuerzos globales en el control nuclear. Su objetivo es evitar la proliferación de armas nucleares y fomentar el desarme nuclear. En 1995, se decidió extender su vigencia indefinidamente, consolidando su importancia en el régimen internacional de no proliferación.
- **Conferencia de Revisión del TNP (2010):** Durante esta conferencia, se adoptó un plan de acción que incluye "13 pasos prácticos relacionados con la no proliferación y el desarme", que abordan cuestiones como la ratificación del Tratado de Prohibición Completa de los Ensayos Nucleares (TPCEN) y la mejora de los mecanismos de verificación nuclear. Aunque este documento estableció un marco ambicioso para avanzar en el desarme, su implementación ha enfrentado desafíos significativos.
- **Tratado sobre la Prohibición de las Armas Nucleares (TPAN):** Adoptado en 2017, este tratado prohíbe completamente las armas nucleares y representa un avance significativo en los esfuerzos por deslegitimar estas armas a nivel global. El TPAN

complementa los esfuerzos existentes bajo el TNP y busca establecer un marco normativo más estricto para el desarme nuclear.

- **Resolución A/RES/67/56**: Esta resolución, adoptada por la Asamblea General de las Naciones Unidas, estableció un grupo de trabajo abierto para desarrollar propuestas que avancen en las negociaciones multilaterales sobre desarme nuclear, buscando lograr un mundo sin armas nucleares

3.6. Expectativas para el debate

Las expectativas para el debate son altas. Se espera que los delegados aborden las crecientes tensiones globales, particularmente entre potencias nucleares como Estados Unidos y Rusia, incrementadas por conflictos recientes como la guerra en Ucrania, lo que ha llevado a una percepción de que el desarme nuclear no es prioritario.

Se espera que también se aborden los obstáculos legales y normativos que impiden un desarme efectivo. La falta de mecanismos de verificación sólidos y la ambigüedad en algunos tratados son problemas importantes que deben abordarse. Los delegados deberán buscar formas de mejorar estos mecanismos y asegurar un cumplimiento más efectivo.

Finalmente, se espera que se reconozca la contribución de organizaciones como la Iniciativa Humanitaria y campañas como ICAN a la promoción del desarme nuclear. Para lograr un mundo con armonía en el tema, será necesaria la presión pública y la movilización internacional, enfocando el debate en promover una conversación constructiva sobre estos temas importantes.

3.7 Recursos Útiles

- https://www.un.org/es/ga/68/meetings/nucleardisarmament/multilateralefforts.shtml

- https://ginhttps://international-review.icrc.org/es/articulos/cambiar-el-discurso-sobre-las-armas-nucleares-la-iniciativa-humanitariaebra-onu.mision.gov.co/desarme
- https://www.impo.com.uy/bases/leyes-internacional/19627-2018/1
- https://www.iaea.org/es/temas/el-oiea-y-el-tratado-sobre-la-no-proliferacion
- https://www.scielo.org.mx/scielo.php?pid=S1870-46542022000100575&script=sci_arttext

4. TEMA B: Las políticas del ciberespacio y los crímenes cibernéticos

4.1 Introducción al tema

Las políticas del ciberespacio y los crímenes cibernéticos son elementos esenciales en el ámbito de la seguridad internacional contemporánea. Con el aumento del uso de Internet, también han proliferado las amenazas digitales, que incluyen delitos como el robo de identidad, el fraude y los ataques de ransomware. Estos crímenes no solo afectan a individuos, sino que también comprometen la seguridad de empresas y naciones enteras.

Las políticas del ciberespacio buscan establecer un marco normativo para combatir estos delitos, pero la rápida evolución de la tecnología y la sofisticación de los ciberdelincuentes presentan desafíos significativos. La cooperación internacional es crucial para abordar estos problemas, ya que los crímenes cibernéticos suelen cruzar fronteras y requieren respuestas coordinadas.

En este contexto, garantizar la seguridad en el ciberespacio implica no solo implementar medidas tecnológicas, sino también desarrollar políticas efectivas y fomentar la colaboración entre países para proteger a todos los actores involucrados en un entorno digital cada vez más complejo.

4.2 Origen

El desarrollo de las políticas del ciberespacio y la respuesta a los crímenes cibernéticos han evolucionado de forma rápida y compleja desde finales del siglo XX, en línea con el avance de la tecnología y el crecimiento del acceso a internet. A medida que esta red se hizo pública en los años 90, surgieron los primeros crímenes en línea, enfocados principalmente en el fraude electrónico, la piratería de software y los virus. En este contexto, las políticas

gubernamentales para el ciberespacio eran casi inexistentes, pues internet se consideraba un ámbito de libre flujo de información con escasa intervención estatal. En respuesta a estos primeros desafíos, la OCDE publicó en 1992 las primeras pautas para la seguridad de sistemas de información, estableciendo una base para futuras normativas.

En la primera década de los 2000, el ciberespacio se expandió a escala global, incrementando tanto la variedad como la complejidad de los crímenes cibernéticos, que pasaron a incluir el robo de identidad, el espionaje industrial y los ataques a infraestructuras críticas. Esto motivó a los gobiernos y organizaciones internacionales a intervenir. En 2001, el Consejo de Europa adoptó la Convención de Budapest, el primer tratado internacional para combatir el cibercrimen, con el fin de criminalizar delitos digitales, facilitar la cooperación internacional y proveer asistencia jurídica transfronteriza. También en esta época, países como Estados Unidos y la Unión Europea crearon agencias como el Departamento de Seguridad Nacional (DHS) y la Agencia de Seguridad de las Redes y de la Información (ENISA) para proteger infraestructuras críticas y responder a incidentes cibernéticos.

La tercera fase de este desarrollo se caracteriza por el surgimiento de la ciberguerra y los conflictos internacionales en el ciberespacio. En esta década, los estados comenzaron a ver internet no solo como un espacio comercial, sino también como un ámbito estratégico para la seguridad nacional, desarrollando capacidades tanto defensivas como ofensivas. Las actividades de espionaje y los ataques patrocinados por estados se volvieron comunes; ejemplos notables incluyen el virus Stuxnet en 2010, que Estados Unidos e Israel habrían usado para frenar el programa nuclear de Irán, y el ataque a la red eléctrica de Ucrania en 2015. La ONU y otros foros internacionales también respondieron: en 2015, establecieron un grupo de trabajo para normar el comportamiento estatal en el ciberespacio y mitigar

conflictos cibernéticos. No obstante, las tensiones geopolíticas han limitado los avances hacia acuerdos vinculantes.

A pesar de estos avances, persisten desafíos importantes, como la falta de consenso sobre la jurisdicción en el ciberespacio y la soberanía digital, así como las limitaciones en la cooperación internacional. Además, la necesidad de equilibrar la seguridad y la privacidad plantea dilemas éticos que deben resolverse conforme evolucionan las amenazas tecnológicas, especialmente con la aparición de nuevas herramientas como la inteligencia artificial y la computación cuántica. En este contexto, la ciberseguridad y el cibercrimen han pasado de ser cuestiones técnicas a temas prioritarios en la política internacional, que requieren de marcos normativos globales y de una cooperación continua para garantizar la seguridad en el ciberespacio.

4.3 Situación actual

La situación actual de las políticas del ciberespacio y de la lucha contra los crímenes cibernéticos plantea múltiples desafíos para el derecho internacional, ya que el rápido avance de la tecnología y la proliferación de delitos en línea requieren de un marco normativo que asegure tanto la protección de derechos como la seguridad en el ámbito digital. En la práctica, los marcos existentes han tenido que adaptarse o evolucionar rápidamente para abarcar problemáticas emergentes, desde el espionaje estatal hasta los ataques cibernéticos a infraestructuras críticas. En este contexto, el derecho internacional se enfrenta a cuestiones sobre soberanía digital, responsabilidad estatal, y la aplicación de principios de jus cogens, es decir, normas imperativas que no admiten derogación y deben ser respetadas por todos los estados.

a. Soberanía y Jurisdicción en el Ciberespacio

Uno de los problemas más complejos en la regulación del ciberespacio es la cuestión de la soberanía. Tradicionalmente, la soberanía territorial ha sido un pilar del derecho internacional, pero el ciberespacio desafía esta noción al trascender fronteras físicas. Esta realidad ha llevado a debates sobre si los estados pueden ejercer un control absoluto sobre su "soberanía digital" en el mismo sentido que lo hacen en sus territorios físicos. La jurisprudencia reciente sugiere una creciente tendencia hacia el reconocimiento de una jurisdicción digital, en la que los estados consideran el acceso a los datos y a las infraestructuras digitales dentro de su territorio como un aspecto de su soberanía.

Por ejemplo, el Reglamento General de Protección de Datos (GDPR) de la Unión Europea, aunque destinado a proteger la privacidad de los ciudadanos europeos, ejerce su alcance extraterritorial al exigir que cualquier empresa que maneje datos de ciudadanos de la UE

cumpla con sus normas, sin importar la ubicación de la empresa. Este ejercicio de extraterritorialidad plantea preguntas en cuanto a la pirámide de Kelsen, que tradicionalmente sitúa las normas internacionales por encima de las nacionales en un sistema jerárquico. Sin embargo, cuando las regulaciones locales como el GDPR imponen obligaciones a actores internacionales, se genera un conflicto entre la autonomía regulatoria de un estado y el principio de no intervención.

b. Normas Imperativas (jus cogens) y Derechos Fundamentales en el Ciberespacio

El derecho internacional en el ciberespacio también requiere que se respeten ciertos principios de jus cogens, como el derecho a la privacidad y a la protección de los derechos humanos fundamentales. La ONU ha afirmado en reiteradas ocasiones que los derechos humanos deben aplicarse igualmente en el entorno digital, como lo establece el Consejo de Derechos Humanos en su resolución 20/8. Sin embargo, el desarrollo de tecnologías de vigilancia masiva, como los sistemas de reconocimiento facial y la recopilación de datos biométricos, plantean serias preocupaciones sobre la violación de estos derechos.

Estados Unidos y otros países han sido criticados por prácticas de espionaje en masa, como las revelaciones de Edward Snowden sobre la Agencia de Seguridad Nacional (NSA) en 2013, que mostró un programa de vigilancia masiva que abarcaba tanto a ciudadanos como a líderes internacionales. Estas prácticas desafían el principium non nocere, un principio ético fundamental que estipula que ningún acto debe causar daño a otros. En este sentido, aunque la seguridad nacional es un objetivo legítimo, debe equilibrarse cuidadosamente con el derecho a la privacidad.

c. Tratados Internacionales y Acuerdos de Cooperación

El marco normativo internacional se ha consolidado en gran parte a través de tratados como la Convención de Budapest sobre Cibercrimen de 2001, que es uno de los pocos acuerdos internacionales específicamente dirigidos a combatir el cibercrimen. Esta convención establece normas de cooperación entre estados y define categorías de delitos, incluyendo la pornografía infantil, el fraude informático, y los ataques a redes de ordenadores. Sin embargo, la Convención de Budapest enfrenta limitaciones importantes, ya que su eficacia depende de la cooperación entre países, y varios estados clave, como China y Rusia, no la han firmado. Estos países argumentan que la convención no respeta plenamente la soberanía nacional, ya que permite a los estados firmantes acceder a datos almacenados en otros territorios sin una autorización previa.

Además, la Resolución 73/27 de la Asamblea General de la ONU de 2018 destaca la importancia de definir normas y principios para una conducta responsable de los estados en el ciberespacio, aunque no es vinculante. Esta resolución llama a los países a abstenerse de actividades que dañen infraestructuras críticas de otros estados, lo cual es fundamental en un contexto donde los ciberataques pueden paralizar sistemas de salud, energía y servicios financieros. A pesar de su naturaleza no vinculante, esta resolución sienta una base para futuras negociaciones multilaterales en el ámbito del ciberespacio.

d. Principios de Responsabilidad Estatal y Acto Ilícito Internacional

El principio de responsabilidad estatal es clave en el derecho internacional para establecer las consecuencias legales cuando un estado actúa de manera que cause daño a otro. En el contexto del ciberespacio, la dificultad de atribuir ataques cibernéticos complica la aplicación de este principio. De acuerdo con el Proyecto de Artículos sobre Responsabilidad de los Estados de la Comisión de Derecho Internacional, un acto ilícito internacional ocurre cuando una conducta atribuible a un estado viola una obligación internacional. Sin embargo, atribuir

un ciberataque a un gobierno específico es complejo debido al uso de técnicas como la falsificación de direcciones IP y la contratación de agentes externos o “cibermilicias”.

La práctica de "atribución de responsabilidad" fue explorada en el Manual de Tallinn, un conjunto de directrices no vinculantes creado por expertos en derecho internacional y ciberseguridad para aplicar el derecho internacional en los conflictos cibernéticos. El Manual establece que un estado víctima de un ciberataque puede ejercer su derecho a defenderse si puede probar con evidencia suficiente que otro estado es responsable del ataque. Sin embargo, el principio de nullum crimen sine lege (no hay crimen sin ley) también complica la respuesta internacional, ya que muchas normas en el ciberespacio aún están en desarrollo, lo cual deja áreas grises en términos de actuación y retaliación.

e. Retos para el Futuro: Gobernanza y Cooperación Internacional

La lucha contra el cibercrimen y la regulación del ciberespacio requieren de una gobernanza multinivel en la que actores estatales, organizaciones internacionales y el sector privado cooperen para establecer estándares de ciberseguridad y respeto a los derechos humanos. La pax digitalis, un concepto emergente, sugiere la necesidad de un ambiente de paz en el ciberespacio que limite las actividades hostiles y garantice una convivencia armónica y segura. Esto implica compromisos éticos y legales de los estados, quienes deben anteponer el bienestar colectivo al interés individual de dominio tecnológico y control.

En este sentido, iniciativas como el Llamado de París para la Confianza y Seguridad en el Ciberespacio, promovido en 2018 por Francia, buscan crear consensos sobre la no proliferación de armas cibernéticas y el respeto a infraestructuras esenciales. Sin embargo, para que estos principios puedan ser efectivos, deben estar respaldados por normas vinculantes y mecanismos de supervisión, ya que el marco actual de "normas voluntarias"

carece de la fuerza coercitiva necesaria para garantizar una seguridad cibernética robusta a nivel global.

En conclusión, la situación actual de las políticas del ciberespacio en el derecho internacional refleja un estado de tensión entre la soberanía estatal, la cooperación global y el respeto a los derechos humanos. Si bien los tratados y principios existentes sientan una base, es fundamental avanzar hacia un sistema regulatorio integral y vinculante que permita enfrentar eficazmente los desafíos del cibercrimen y la ciberguerra. A medida que la tecnología continúa transformándose, el derecho internacional debe adaptarse rápidamente para proteger a individuos y estados en un entorno digital cada vez más interconectado.

4.4 Resoluciones previas

Resolución 55/63 (2000): "Combate contra el uso de tecnologías de la información con fines delictivos"

- Reconoce el impacto del cibercrimen en la seguridad de los estados e insta a fortalecer los marcos legales nacionales y la cooperación internacional.

Resolución 64/211 (2009): "Fortalecimiento de la seguridad en la información y ciberseguridad"

- Introduce el concepto de "seguridad en la información" en el contexto internacional y llama a desarrollar legislaciones nacionales para abordar los ciberataques.

Resolución 68/167 (2013): "El derecho a la privacidad en la era digital"

- Resalta la obligación de los estados de proteger la privacidad y los datos personales en el ciberespacio, en conformidad con derechos reconocidos internacionalmente.

Resolución 73/27 (2018): "Avances en la informática y la telecomunicación en el contexto de la seguridad internacional"

- Insta a los países a abstenerse de realizar ataques cibernéticos contra infraestructuras críticas y promueve la confianza y transparencia entre estados en el ciberespacio.

Resolución 74/247 (2019): "Contrarrestar el uso de las tecnologías de la información y las comunicaciones con fines delictivos"

- Establece un comité para desarrollar un tratado contra el cibercrimen y destaca la importancia de la cooperación técnica y la protección de derechos humanos en políticas de ciberseguridad.

Resolución 75/282 (2021): "Convención sobre la Ciberdelincuencia"

- Inicia el proceso para negociar una convención internacional contra el cibercrimen, con el objetivo de facilitar la cooperación y proteger los derechos humanos en el ciberespacio.

4.5 Expectativas de debate

Las expectativas para el debate son grandes. Se espera que los delegados aborden las crecientes tensiones globales, especialmente en torno a las disputas de ciberseguridad entre potencias, exacerbadas por recientes ciberataques y conflictos geopolíticos que han puesto en evidencia la vulnerabilidad de las infraestructuras digitales críticas y la falta de consenso sobre normativas en el ciberespacio.

También se anticipa que se traten los complejos obstáculos legales y normativos que dificultan una cooperación internacional efectiva en la prevención y persecución del cibercrimen. La falta de un marco jurídico global vinculante, las diferencias en las legislaciones nacionales y la ambigüedad en algunos acuerdos internacionales son cuestiones clave que los delegados deberán analizar. Será fundamental explorar soluciones para fortalecer los mecanismos de cooperación y establecer pautas claras de jurisdicción y responsabilidad en el ciberespacio.

Finalmente, se espera que los delegados reconozcan el rol de iniciativas y organizaciones internacionales que promueven la regulación del ciberespacio y la ciberseguridad, así como de campañas de sensibilización pública que llaman a una mayor protección de los derechos digitales y a una regulación ética del entorno digital. Para avanzar hacia un consenso global en estos temas, será esencial la movilización y presión internacional que aliente un debate constructivo y orientado a soluciones duraderas.

4.6 Recursos Útiles

- https://www.scielo.cl/scielo.php?pid=S0719-25842019000200001&script=sci_arttext
- https://obtienearchivo.bcn.cl/obtienearchivo?id=repositorio%2F10221%2F30304%2F1%2FPoliticas_de_ciberseguridad_en_la_experiencia_internacional.pdf
- https://digital-strategy.ec.europa.eu/es/policies/cybersecurity-policies
- https://www.oas.org/es/sla/cji/docs/Derecho_Internacional_y_Operaciones_Cibern%C3%A9ticas_del_Estado_publicacion.pdf
- https://www.redalyc.org/journal/531/53163845010/html/

- https://www.diplomatie.gouv.fr/es/politica-exterior/seguridad-desarme-y-no-proliferacion/ciberseguridad/
- https://es.weforum.org/stories/2015/05/una-normativa-internacional-para-el-ciberespacio/

5. QARMAS

5.1 TEMA A

- ¿Cuál es la posición de su país respecto a la extensión o modificación del Tratado de No Proliferación Nuclear (TNP)?
- ¿Cómo propone su país abordar el desafío de los actores no estatales en el contexto de la no proliferación de armas?
- ¿Cuál es la postura de su país sobre la creación de zonas libres de armas nucleares en regiones específicas?
- ¿Qué medidas recomienda su delegación para mejorar la transparencia y la confianza entre los estados en materia de desarme?
- ¿Qué papel considera su delegación que deben jugar las organizaciones regionales en el fortalecimiento de los regímenes de desarme?

5.2 TEMA B

- ¿Qué medidas específicas propone su país para fomentar la cooperación internacional en la lucha contra la ciberdelincuencia?
- ¿Cómo aborda su delegación la cuestión de la protección de datos y la privacidad en el contexto de las políticas del ciberespacio?
- ¿Qué iniciativas recomienda su delegación para mejorar la transparencia y el intercambio de información entre países sobre amenazas cibernéticas?
- ¿Qué acciones ha tomado su gobierno para fortalecer las capacidades nacionales en materia de respuesta a incidentes cibernéticos?
- ¿Cuáles son las estrategias que su delegación apoya para educar a los ciudadanos sobre los riesgos y amenazas cibernéticas?

6. Delegaciones

1. Estados Unidos
2. Rusia
3. China
4. Reino Unido
5. Francia
6. India
7. Japón
8. Alemania
9. Israel
10. Corea del Norte
11. Irán
12. Pakistán
13. Brasil
14. Canadá
15. Australia
16. Arabia Saudita
17. Turquía
18. Ucrania
19. Egipto
20. Sudáfrica
21. Singapur
22. Emiratos Árabes Unidos
23. Italia
24. España
25. México

7. Bibliografía

- Council of Europe. (2001). Convention on Cybercrime. https://www.coe.int/en/web/cybercrime/the-budapest-convention
- Gordon, S. J., & Ford, W. F. (2006). A framework for understanding cyber crime. Computers & Security, 25(3), 224-229. https://doi.org/10.1016/j.cose.2005.12.002
- Kerr, O. S. (2018). The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution. Harvard Law Review, 102(4), 105-123. https://www.jstor.org/stable/1342345
- Nissenbaum, H. (2010). Privacy in Context: Technology, Policy, and the Integrity of Social Life. Stanford University Press.
- United Nations Office on Drugs and Crime (UNODC). (2013). Comprehensive Study on Cybercrime. https://www.unodc.org/documents/organized-crime/Cybercrime_Study_2013.pdf
- Zittrain, J. L. (2008). The Future of the Internet and How to Stop It. Yale University Press.
- Holt, T. J., & Bossler, A. M. (2008). Examining the relationship between cyber crime and traditional crime: A review of the literature. Journal of Criminal Justice, 36(4), 365-376. https://doi.org/10.1016/j.jcrimjus.2008.06.001
- International Telecommunication Union (ITU). (2018). Global Cybersecurity Index. https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx
- European Union Agency for Cybersecurity (ENISA). (2020). Threat Landscape for Cybersecurity in 2020. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2020
- Pew Research Center (2017). The Future of Cybersecurity: Experts' Predictions for 2025. https://www.pewresearch.org/internet/2017/05/03/the-future-of-cybersecurity/