DISEC.

Desarme y seguridad internacional.

JOSMUN 2025

Mesa:

Jeronimo Lozano Velásquez

Juan David Escobar

Tema A: Regulación de los ataques cibernéticos y el comercio ilegal de datos privados hacia personas jurídicas.

Tema B: Regulación del uso de las inteligencias artificiales como utensilio militar y cómo ayudantes para la innovación de armamento nuclear.

TABLA DE CONTENIDOS

1. Carta de presidentes.

Estimados delegados.

Es un honor para nosotros darles la bienvenida a la XIII versión de JOSMUN, en especial al comité de la Primera Comisión de Desarme y Seguridad Internacional (DISEC). Durante este evento, tendrán la oportunidad de abordar algunos de los desafíos más urgentes en materia de seguridad global, desde la proliferación de armas hasta el impacto de los avances tecnológicos en los conflictos internacionales.

DISEC representa un espacio donde la diplomacia y la estrategia se entrelazan para buscar soluciones sostenibles y viables a problemas que afectan la paz y la estabilidad mundial. A lo largo de las sesiones, esperamos que pongan en práctica sus habilidades analíticas y de negociación, enfrentando los retos con creatividad, argumentación sólida y un compromiso genuino con el debate constructivo.

Entendemos que la preparación y el desarrollo de los debates pueden resultar exigentes, pero queremos recordarles que cuentan con nuestro apoyo en todo momento. Como sus presidentes, estamos aquí para guiarlos, responder sus dudas y asegurarnos de que esta experiencia sea enriquecedora y gratificante para todos.

Aprovechen al máximo esta oportunidad para aprender, compartir ideas y construir soluciones que reflejen la importancia del multilateralismo en la búsqueda de la paz. Agradecemos su confianza en nuestro trabajo y estamos seguros de que juntos haremos de este comité un espacio de diálogo significativo y aprendizaje.

Atentamente,

Jerónimo Lozano y Juan David

Presidentes del comité DISEC

2. Introducción al comité DISEC

La Primera Comisión de Desarme y Seguridad Internacional (DISEC) de las Naciones Unidas es un órgano clave en la promoción de la paz y la estabilidad global. Su principal objetivo es debatir y formular recomendaciones sobre temas relacionados con el desarme, la regulación del uso de armamento y la seguridad internacional. A través del diálogo diplomático, DISEC busca fortalecer la cooperación entre los Estados para prevenir conflictos y garantizar el respeto al derecho internacional en materia de defensa y seguridad.

En esta edición de JOSMUN, abordaremos dos problemáticas cruciales para la seguridad global:

1. Regulación de los ataques cibernéticos y el comercio ilegal de datos privados hacia personas jurídicas. En un mundo cada vez más digitalizado, la ciberseguridad se ha convertido en una prioridad internacional. Analizaremos cómo los Estados pueden enfrentar las amenazas cibernéticas, prevenir la vulneración de información sensible y fortalecer mecanismos de cooperación para combatir el comercio ilegal de datos privados.

2. Regulación del uso de las inteligencias artificiales como utensilio militar y cómo ayudantes para la innovación de armamento nuclear. La evolución de la inteligencia artificial (IA) plantea desafíos éticos y estratégicos en el ámbito militar. Discutiremos los límites del uso de la IA en la guerra, los riesgos de su implementación en armas autónomas y

su posible papel en el desarrollo de armamento nuclear, con el fin de establecer regulaciones que equilibren la innovación con la seguridad global.

A lo largo de este comité, los delegados deberán analizar estos temas desde una perspectiva crítica y estratégica, proponiendo soluciones viables que garanticen la seguridad internacional sin comprometer el desarrollo tecnológico. Los invitamos a participar con compromiso, argumentación fundamentada y un enfoque diplomático, contribuyendo así a la construcción de un mundo más seguro y estable.

2.1 objetivos y funciones

La Primera Comisión de Desarme y Seguridad Internacional (DISEC) de las Naciones Unidas, en el marco de JOSMUN, tiene como objetivo promover la paz, la seguridad y la estabilidad global mediante el diálogo diplomático y la cooperación entre los Estados. Su labor principal es analizar y formular recomendaciones sobre temas relacionados con el desarme, la regulación de armamentos y la seguridad internacional. En esta edición, el comité enfocará su trabajo en dos problemáticas fundamentales: la regulación de los ataques cibernéticos y el comercio ilegal de datos privados hacia personas jurídicas, así como la regulación del uso de inteligencias artificiales como utensilios militares y como asistentes en la innovación de armamento nuclear. Entre sus funciones, DISEC debe fomentar el debate crítico y estratégico sobre estos temas, formular propuestas viables que permitan enfrentar las amenazas emergentes respetando el derecho internacional, y promover marcos de cooperación internacional que fortalezcan la prevención de conflictos. Además, los delegados deberán diseñar resoluciones que equilibren el avance tecnológico con la necesidad de garantizar la seguridad global, estableciendo límites éticos y jurídicos para el uso de nuevas tecnologías en el ámbito militar. Con compromiso, fundamentación y diplomacia, el comité busca contribuir a la construcción de un mundo más seguro y estable para todos.

3. funcionamiento del club.

3.1 Funcionamiento del comité.

El comité de Desarme y Seguridad Internacional (DISEC) funciona como un espacio diplomático de análisis, negociación y propuesta dentro de la estructura de las Naciones Unidas, teniendo como mandato abordar cuestiones fundamentales relacionadas con la reducción de armamentos y el fortalecimiento de la paz mundial. En sus sesiones, los delegados de cada Estado miembro debaten activamente sobre temas emergentes que amenazan la seguridad global, como los conflictos armados, el tráfico ilícito de armas, las nuevas tecnologías militares y los ciberataques. Las decisiones de DISEC no tienen un carácter vinculante, pero sus recomendaciones y resoluciones orientan las políticas internacionales y sirven como base para futuros tratados o acciones de la comunidad internacional. Durante el desarrollo del comité, se siguen procedimientos formales que incluyen la apertura de debates, la exposición de posturas nacionales, la formación de bloques de negociación, la elaboración de borradores de resoluciones y finalmente la votación de los documentos que reflejan los consensos alcanzados. La dinámica de trabajo se caracteriza por la búsqueda constante de soluciones equilibradas que respeten los intereses de los Estados, sin comprometer los principios del derecho internacional humanitario ni la estabilidad global. DISEC actúa, por tanto, como un puente entre el progreso tecnológico y la responsabilidad colectiva, impulsando un diálogo que permita anticipar riesgos y promover un entorno de seguridad más sólido para las generaciones futuras.

4. Tema A: regulación de los ataques cibernéticos y el comercio ilegal de datos privados hacia personas jurídicas.

4.1 introducción al tema A.

El crecimiento exponencial de la tecnología y la digitalización de los procesos comerciales han traído consigo una mayor exposición a riesgos cibernéticos. Las personas jurídicas, incluidas empresas, instituciones gubernamentales y organizaciones sin ánimo de lucro, se han convertido en objetivos principales de ataques cibernéticos. Estos ataques buscan vulnerar sistemas informáticos para robar información confidencial, causar daño operativo o lucrarse mediante el comercio ilegal de datos privados.

A lo largo de los años, la seguridad cibernética ha evolucionado en un intento de proteger a las organizaciones de estos ataques, pero los ciberdelincuentes han desarrollado técnicas cada vez más sofisticadas. Ante esta problemática, las regulaciones en torno a la protección de datos y la persecución de delitos informáticos han cobrado una importancia fundamental. Sin embargo, la globalización de Internet y la diversidad de marcos jurídicos entre los países dificultan la aplicación efectiva de leyes internacionales, lo que deja brechas de seguridad que son aprovechadas por actores malintencionados.

4.2 contexto histórico.

Los delitos cibernéticos han existido desde el inicio de la informática conectada a redes, pero su impacto se hizo más evidente con la masificación de Internet en la década de 1990. En ese

período, surgieron los primeros virus y troyanos diseñados para infiltrarse en sistemas, así como los ataques de denegación de servicio (DDoS), que saturaban servidores y provocan caídas de plataformas.

Uno de los primeros intentos de regulación internacional se dio con la Convención de Budapest sobre Ciberdelincuencia (2001), el primer tratado internacional que abordó delitos informáticos y la cooperación judicial entre países para combatirlos. No obstante, el crecimiento del comercio digital y la dependencia de la nube trajeron nuevos desafíos.

En los años 2010, con la proliferación de redes sociales y plataformas de comercio electrónico, la recolección masiva de datos se convirtió en una práctica común. Esta información, en muchos casos, fue vulnerada por ciberdelincuentes que encontraron en el robo y venta de datos una fuente lucrativa. Los gobiernos y las empresas comenzaron a implementar regulaciones más estrictas, como el Reglamento General de Protección de Datos (GDPR) de la Unión Europea, aprobado en 2016 y en vigor desde 2018.

A pesar de estos avances, el cibercrimen ha seguido evolucionando, con ataques más sofisticados y difíciles de rastrear. La falta de un marco legal global uniforme ha permitido que organizaciones criminales operan desde países con regulaciones débiles o nulas sobre ciberdelitos.

4.3 situación actual

En la actualidad, la ciberseguridad se ha convertido en una de las principales preocupaciones tanto de gobiernos como de empresas privadas. Los ataques cibernéticos no solo han aumentado en número, sino también en sofisticación, afectando a una amplia gama de objetivos que incluyen desde pequeñas empresas hasta grandes corporaciones tecnológicas y

entidades gubernamentales críticas. Estos ataques pueden tener consecuencias devastadoras, como pérdidas económicas multimillonarias, robo de información confidencial y amenazas a la infraestructura nacional, incluyendo sectores estratégicos como la energía, la salud y la banca.

Para enfrentar estos desafíos, varios gobiernos han implementado regulaciones específicas que buscan proteger la información y reforzar los sistemas de defensa cibernética. Entre ellas destacan la **California Consumer Privacy Act (CCPA)** en Estados Unidos, enfocada en la protección de datos personales de los consumidores, la **Ley de Ciberseguridad de China** (2017), que establece estrictos requisitos de almacenamiento de datos y control estatal sobre la información, y legislaciones nacionales como la **Ley Federal de Protección de Datos en Alemania**, el **Reglamento General de Protección de Datos (GDPR)** en el Reino Unido (durante su permanencia en la Unión Europea) y la **Ley General de Protección de Datos Personales (LGPD)** en Brasil. No obstante, las diferencias en los enfoques regulatorios, las prioridades nacionales y los niveles de cumplimiento dificultan la posibilidad de una respuesta coordinada a nivel internacional frente a las amenazas cibernéticas.

A este panorama se suma el crecimiento del comercio ilegal de datos, que opera principalmente a través de la **deep web** y mercados clandestinos. En estos espacios, se trafican bases de datos que contienen información sensible de usuarios, contraseñas, números de tarjetas de crédito y registros médicos, alimentando una industria clandestina sumamente lucrativa. La falta de mecanismos internacionales efectivos para rastrear, desmantelar y sancionar estas redes de ciberdelincuencia representa una de las principales vulnerabilidades del sistema de ciberseguridad global actual. Esta realidad resalta la urgente necesidad de fortalecer la cooperación internacional, armonizar las normativas y establecer marcos

comunes de acción que permitan proteger de manera efectiva la información en el mundo digital.

4.4 consecuencias.

Los ataques cibernéticos y el comercio ilegal de datos tienen repercusiones significativas en distintos niveles:

- Económicas: Las empresas pueden sufrir pérdidas millonarias debido a robos financieros, demandas por filtración de datos y gastos en recuperación de sistemas. Según estudios, el costo promedio de una filtración de datos es de varios millones de dólares.

- Legales: La exposición de datos privados puede derivar en sanciones a las empresas que no cumplan con normativas de protección de datos, además de posibles acciones legales por parte de clientes afectados.

- Reputacionales: Las empresas que sufren filtraciones masivas de datos pueden perder la confianza de sus clientes, lo que impacta directamente en su credibilidad y valor de mercado.

- Operativas: Un ataque exitoso puede paralizar operaciones clave, comprometer secretos comerciales y poner en riesgo la estabilidad de una empresa.

4.5 casos importantes.

- Equifax (2017): La agencia de crédito estadounidense sufrió una brecha que expuso la información de 147 millones de personas, incluyendo números de seguridad social y datos financieros.

- Yahoo (2013-2014): Un ataque masivo comprometió la seguridad de 3.000 millones de cuentas de usuarios, siendo uno de los incidentes más grandes en la historia de Internet.

- SolarWinds (2020): Un ataque de espionaje cibernético permitió a hackers infiltrarse en agencias gubernamentales y empresas privadas de EE. UU., aprovechando vulnerabilidades en el software de la compañía.

Facebook (2019) – Filtración de datos de 530 millones de usuarios, incluyendo teléfonos y correos electrónicos, publicados en foros de hackers.

2. Marriott International (2018) – Brecha que afectó a 500 millones de clientes, exponiendo nombres, pasaportes y tarjetas de crédito.

3. Sony Pictures (2014) – Hackeo que filtró correos internos y películas inéditas. Se sospecha de la participación de Corea del Norte.

4.6 subtemas de interés.

1. Normativas internacionales y su eficacia: Evaluación de tratados y leyes existentes para combatir ataques cibernéticos.

2. Impacto del cibercrimen en la economía global: Análisis de cómo los ataques afectan mercados y estabilidad financiera.

3. Ética y legalidad en la recolección y venta de datos: Discusión sobre los límites de la recopilación de datos por parte de empresas tecnológicas.

4. Uso de inteligencia artificial en ciberseguridad: Cómo la IA puede ayudar a detectar y prevenir ataques.

5. Responsabilidad corporativa en la protección de datos: Obligaciones de las empresas para garantizar la seguridad de su información y la de sus clientes.

4.7 preguntas a los delegados

1. ¿Qué regulaciones existen en su país para prevenir ataques cibernéticos contra empresas?

2. ¿Cómo pueden fortalecerse las medidas internacionales contra el comercio ilegal de datos?

3. ¿Qué papel juegan las empresas tecnológicas en la protección de la información de las personas jurídicas?

4. ¿Es suficiente la legislación actual o se requieren enfoques más estrictos?

5. ¿Qué medidas pueden adoptar las empresas para mejorar su ciberseguridad?

6. ¿Cómo pueden los países cooperar para rastrear y sancionar a los ciberdelincuentes que operan a nivel global?

4.8 recomendaciones de la mesa

1. Fortalecer la cooperación internacional en ciberseguridad, promoviendo tratados y acuerdos vinculantes.

2. Implementar sanciones más severas para ciberdelincuentes y empresas negligentes en la protección de datos.

3. Fomentar la inversión en tecnología de seguridad, incluyendo IA y blockchain para proteger información sensible.

4. Establecer estándares globales de seguridad informática, asegurando que todas las empresas cumplan con medidas mínimas de protección.

5. Promover la educación y concienciación en ciberseguridad dentro de organizaciones, para evitar errores humanos que faciliten ataques.

Estas medidas buscan fortalecer la seguridad digital de las personas jurídicas y reducir los riesgos asociados a los ataques cibernéticos y el comercio ilegal de datos.

5. referencias.

http://www.ordenjuridico.gob.mx/Congreso/pdf/133.pdf

https://www.ftc.gov/es/guia-para-negocios/como-proteger-la-informacion-personal-una-guia-para-negocios

https://www.oas.org/juridico/spanish/cyb_ecu_delitos_inform.pdf

https://www.boe.es/buscar/act.php?id=BOE-A-2021-1192

https://www.unodc.org/e4j/es/cybercrime/module-8/key-issues/international-cooperation-on-cybersecurity-matters.html

https://www.aepd.es/guias/guia-brechas-seguridad.pdf

California Consumer Privacy Act (CCPA): https://oag.ca.gov/privacy/ccpa

Ley de Ciberseguridad de China (2017):

https://www.chinalawtranslate.com/en/cybersecuritylaw/

GDPR - Reglamento General de Protección de Datos (referido al Reino Unido antes del Brexit): https://gdpr-info.eu/

Ley General de Protección de Datos Personales (LGPD) - Brasil:

https://www.gov.br/cidadania/pt-br/acesso-a-informacao/lgpd

Información sobre comercio ilegal de datos en la deep web: reportes de Europol (por ejemplo, el "Internet Organised Crime Threat Assessment" - IOCTA 2023):

https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2023

4. Tema B: Regulación de la IA en el ámbito militar y su impacto en el

desarrollo de armas nucleares

4.1 Introducción al tema B

En el sector militar, en el avance de las armas nucleares, la inteligencia artificial (IA) ha obtenido mayor relevancia. Los avances de la IA han permitido su aplicación en temas de vigilancia, drones autónomos y análisis de información, sin embargo también enfrenta desafíos éticos y legales. La autonomía en sistemas de seguridad genera preocupación sobre la responsabilidad y los riesgos en aumento, mientras que la protección de estos sistemas se podría romper con ataques cibernéticos. No obstante de que las leyes internacionales abarcan normas para el uso de fuerza, no hacen referencia específica a la IA, lo que ha causado esfuerzos internacionales para establecer normas para su empleo seguro en escenarios militares

4.2. Contexto histórico

La historia del uso de inteligencia artificial (IA) en campos de guerra cubre varios años, desde los primeros equipos usados en la Segunda Guerra Mundial hasta los sistemas modernos de aprendizaje mático. Desde ese tiempo la Inteligencia Artificial ha tenido una gran evolución, pasando de ser un herramienta más para romper códigos y ver datos a vueltas hacerse una parte clave en las estrategias militares actuales. Este cambio ha tenido avances tecnológicos grandes, cambios geopolíticos y charlas éticas sobre el papel de la autonomía en conflicto bélico.

4.2.1. Acontecimientos

● Post-Segunda Guerra Mundial (1945): El uso de armas nucleares en Hiroshima y Nagasaki (1945) que fue un momento histórico marcó el fin de la segunda guerra mundial, pero le dió inicio a la era nuclear y generó preocupación global sobre su control.

● Incidente del Equinoccio de Otoño: En la década de 1980, la automatización de ciertos procesos de lanzamiento generó preocupaciones sobre el funcionamiento de dispositivos de detección automatizados, como el incidente de Stanislav Petrov en 1983, donde el sistema de detección de misiles creado por la Unión Soviética detectó erróneamente sobre un ataque desde EEUU, pero milagrosamente el oficial Stanislav Petrov no informó a sus superiores y pudo evitar una guerra nuclear entre estas dos naciones

● Uso Estadounidense: Estados Unidos empezó a abrir paso la IA de lleno durante la guerra del golfo (1991) para la planificación de logística, sistemas de navegación y análisis de datos. Con el tiempo él mismo empezó a emplear la inteligencia artificial para desarrollar defensas antimisiles y en los 90s empezaron a emplear nuevas aplicaciones como drones desarrollados con IA rudimentaria para el reconocimiento y vigilancia.

4.2.2. Tratados, iniciativas, declaraciones y acuerdos

● Tratado de No Proliferación Nuclear (TNP, 1968): El tratado de la no proliferación nuclear es un tratado negociado bajo el marco de las Naciones Unidas firmado en 1968, entrando en vigor en 1970, ratificado por 191 países. Este tratado surgió debido a la carrera armamentística de aquel entonces y era requerido para no multiplicar el surgimiento de utensilios nucleares, también para promover el uso pácifico de energía nuclear. El tratado fue mayormente impulsado por Estados Unidos y la Unión Soviética (URSS), seguido por Reino Unido, China y Francia. Pero naciones tales como: India, Pakistán e Israel decidieron no

hacer parte de este. Y el caso específico de Corea del Norte que se unió al tratado en 1985, pero este se retiró del tratado en el año 2003.

● Convención sobre Ciertas Armas Convencionales (CCW, 1980): El tratado de convección de ciertas armas convencionales, conocido como "tratado Convención de Ginebra sobre Armas Inhumanas" es un tratado emergente de 1980 que entró en vigor en el año 1983 para la prohibición o restricción sobre el uso de armas que causen daños excesivos o efectos indiscriminados. Este emergió para regular el uso de nuevas tecnologías emergentes en el ámbito bélico, protección humanitaria y la creación de Principios del derecho internacional humanitario que son: la distinción entre civiles y combatientes, y la prohibición del empleo de armas que causen males superfluos o sufrimientos innecesarios

● Tratado INF (Fuerzas Nucleares de Rango Intermedio, 1987-2019): El tratado de Fuerzas Nucleares de Rango Intermedio es un acuerdo entre Estados Unidos y la Unión Soviética para la eliminación de misiles nucleares de rango intermedio, dando fin a la crisis de los euromisiles y sentando la base para los tratados START. Este tratado tuvo su ruptura en 2019, ya que EEUU y la OTAN acusan a Rusia de haber violado este tratado.

● Tratados START (Reducción de Armas Estratégicas, 1991): Los tratados START son tratados entre EEUU y Rusia donde se acuerdan reducciones y limitaciones de armas nucleares estratégicas.

● Tratado de Prohibición Completa de los Ensayos Nucleares (TPCEN, 1996): El tratado de prohibición completa de los ensayos nucleares es un tratado aprobado por la asamblea general de la ONU, firmado por países tales como: EEUU, China, Rusia, Francia y Reino Unido. Pero estas y demás naciones como Pakistán, Corea del Norte, Israel, Irán, Egipto, E.T.C no han ratificado este tratado impidiendo el vigor de este

● Principios de Asilomar sobre IA (2017): Los principios de Asilomar formulados en 2017 son principios de investigación,problemáticas a largo plazo, ética y valores. Los principales actores son figuras como Elon Musk, Stephen Hawking, Stuart Russell, Nick Bostrom, Max Tegmark y demás científicos y expertos en el área.

4.3 situación actual.

En los últimos años, el empleo de inteligencia artificial (IA) en el ámbito militar ha presentado un aumento significativo, con la creación de armas de funcionamiento autónomo y sistemas de cuidado en línea guiados por programas automáticos. Naciones tales como Estados Unidos, China y Rusia han invertido capital en la inteligencia artificial para potencializar la precisión y rapidez en casos bélicos.

● China: El presidente Xi Jinping llegó a un acuerdo con el expresidente de EE.UU, Joe Biden donde se comprometen a hacer el uso responsable del uso de IA . A pesar de esto China se encuentra activamente desarrollando armas militares como robots armados, tanques, barcos y drones con impulso de inteligencia artificial, esto con la intención de convertirse en líder mundial en IA para el año 2030.

● Estados Unidos: Por otro lado EE.UU crea alianza con OpenAI y laboratorios nacionales con el objetivo de acelerar el desarrollo científico, mejorar la seguridad nuclear y reforzar la ciberseguridad de infraestructuras críticas con la intención de mantener su supremacía y contener a naciones tales como China y Rusia.

● Rusia: Rusia lleva poco más de una década estudiando y aplicando la IA llamada el proyecto Steelers que tiene como objetivo el desarrollo de conjuntos de software y hardware de alta confianza que ha sido usado en conflictos regionales como lo han sido con naciones

tales como Siria y Ucrania. También está formó alianzas con China, donde buscan fortalecer sus capacidades tecnológicas y desafiar a Estados Unidos.

● Unión Europea: La UE busca convertirse en un líder mundial en IA segura y confiable. Por esto han lanzado la ley de IA que plantea un marco regulatorio para garantizar que los sistemas de IA sean seguros, transparentes, éticos e imparciales para poder hacer uso de esta en áreas como la salud, el transporte, la energía y la manufactura

Según la organización "RAND" sus investigaciones realizadas por medio de talleres con expertos de la IA y seguridad nuclear, afirma: *"la IA tiene el potencial de exacerbar los desafíos emergentes para la estabilidad estratégica nuclear para el año 2040, incluso con tasas modestas de progreso técnico. Por lo tanto, es importante entender cómo podría suceder esto y asegurar que no lo haga.es importante entender cómo podría suceder esto y asegurar que no lo haga.es importante entender cómo podría suceder esto y asegurar que no lo haga.*" Para la ONU a finales de 2024 este tema ya generó preocupación y su Secretario General, António Guterres, advirtió sobre los riesgos de la inteligencia artificial (IA) y urgió a la acción internacional para prevenir su uso indebido, especialmente en la paz y seguridad globales. Guterres señaló que el rápido desarrollo de la IA está superando nuestra capacidad para gobernarla, planteando preguntas fundamentales sobre responsabilidad, igualdad, seguridad y protección. Guterres describió la integración de la IA con las armas nucleares como "particularmente alarmante" y advirtió sobre las consecuencias potencialmente catastróficas, y dijo que "debemos evitarlo a toda costa". Destacó la importancia de mantener el control humano en la toma de decisiones, y urgió a la adhesión a las leyes internacionales y los principios éticos. También propuso establecer un Panel Científico Internacional sobre la IA y lanzar un Diálogo Global sobre la Gobernanza de la IA.

4.7 preguntas a los delegados.

1. ¿Cómo se debe regular la inteligencia artificial en el contexto militar para prevenir amenazas estratégicas y humanitarias?

2. ¿Qué repercusión es considerada para que la aplicación de Inteligencia Artificial en sistemas de seguridad nuclear tendría en la estabilidad mundial y la seguridad a nivel internacional?

3. ¿Está su delegación abierta a fin de aceptar regulaciones en la utilización de Inteligencia Artificial militar si esto reduce la posibilidad de ascensos accidentales en conflictos internacionales?

4. ¿Qué medidas se pueden implementar para garantizar que la regulación de la Inteligencia Artificial en la defensa militar no dañe la soberanía de los países con menor capacidad tecnológica?

5. ¿De qué manera puede su delegación aportar al consolidación de marcos jurídicos que eviten la utilización inapropiada de IA en conflictos bélicos?

6. ¿De qué manera puede la ONU fortalecer los sistemas de comprobación y control para asegurar que la implementación de IA en sistemas de defensa nuclear sea segura y responsable?

7. ¿De qué manera los países en vías de desarrollo pueden involucrarse en las decisiones relacionadas con la regulación de la IA en defensa sin quedarse atrasados respecto a las potencias tecnológicas?

8. ¿Cómo se puede evitar que la aplicación de Inteligencia Artificial en el sector militar debilite las bases de disuasión y estabilidad estratégica entre las naciones?

9. ¿De qué manera están evaluando los beneficios y riesgos de la Inteligencia Artificial en el sector militar para asegurar la seguridad internacional?

10. ¿De qué manera se está fomentando a nivel internacional la educación y formación en ética de la Inteligencia Artificial para los creadores y operadores de sistemas bélicos?

4.8. Recomendaciones de la mesa.

La finalidad de esta guía de estudio es brindar todas las herramientas necesarias para entender el tema sin requerir tiempo en fuentes adicionales; sin embargo, es fundamental analizar correctamente la realidad contextual en diversos aspectos, incluyendo la realidad contextual en distintos aspectos. La gestión de la política exterior, las normativas jurídicas internas, y otros elementos relacionados con la delegación individual otorgada y la resolución de los problemas que serán los instrumentos guías del comité, por lo que su evolución será constante. específicamente relevante. En este entorno de discusión de ideas, se les invita a ser muy creativos. participativos y a aprovechar al máximo la experiencia, ya que todos tendrán la misma. oportunidad de aprendizaje, así que cualquier esfuerzo realizado por ustedes será satisfactorio. Es crucial que las delegaciones, al elaborar una resolución, sean innovadoras y conserven consistencia tanto con la realidad global como con las metas de la comisión. Es crucial superar discrepancias y lograr pactos equitativos que tomen en cuenta los diferentes contextos para establecer los términos que guiarán las posibles soluciones a la problemática

en debate. Como es un asunto extenso, contemporáneo y de compleja solución, resultará crucial incorporar contribuciones que potencien el debate y ayuden a su tratamiento. Para finalizar. Como expresó el empresario Andrew Carnegie: "No serás un gran líder si quieres hacer todo por ti mismo o solo obtener el crédito de ello". Los animamos a promover la cooperación dentro de la comisión, dado que una de las competencias más cruciales de un delegado es la habilidad para negociar e involucrarse, en conjunto, en la creación de soluciones conjuntas. En última instancia, la unidad ha sido y continuará siendo el factor crucial para el avance de la humanidad.

5. Referencias:

Army University Press. (2010). La guerra en el siglo XXI: una perspectiva del conflicto futuro. https://www.armyupress.army.mil/Portals/7/military-review/Archives/Spanish/MilitaryReview_20100831_art006SPA.pdf

Aydogan, M. (2024). UN chief urges global action to address AI's threats to peace, security. https://www.aa.com.tr/en/world/un-chief-urges-global-action-to-address-ais-threats-to-peacesecurity/3429323

Comisión Europea. (s.f.). Excelencia y confianza en la inteligencia artificial. https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/excellence-and-trust-artificial-intelligence_es

El Confidencial. (2017, febrero 2). Elon Musk, Stephen Hawking y la inteligencia artificial: "Puede ser nuestra mayor hazaña o nuestro peor error".

https://www.elconfidencial.com/tecnologia/2017-02-02/inteligencia-artificial-elon-musk-stephen-hawking-ia_1325057/

Edward, G., & Lohn, A. J. (2018). How might artificial intelligence affect the risk of nuclear war? | RAND. https://www.rand.org/pubs/perspectives/PE296.html

Fried, I. (2025, enero 30). OpenAI, Microsoft y Sam Altman: Colaboración en Los Álamos para avances científicos. Axios. https://www.axios.com/2025/01/30/openai-microsoft-sam-altman-los-alamos-science

Müller, D. N. (2023, octubre 7). Archivos militares secretos: así utiliza Rusia la inteligencia artificial para sus misiles nucleares. Business Insider España. https://www.businessinsider.es/politica/utiliza-rusia-inteligencia-artificial-misiles-nucleares-1316058

Naciones Unidas. (2023, agosto 4). El uso de la inteligencia artificial en el ámbito militar debe regularse, advierte Guterres. https://news.un.org/es/story/2023/08/1523652

National Geographic. (2024, agosto 6). Hiroshima y Nagasaki: la masacre de las bombas atómicas. https://historia.nationalgeographic.com.es/a/hiroshima-nagasaki-masacre-bombas-atomicas_10590

National Security Archive. (2019, agosto 2). INF Treaty, 1987-2019. https://nsarchive.gwu.edu/briefing-book/russia-programs/2019-08-02/inf-treaty-1987-2019

Notigram. (2024, noviembre 16). Joe Biden y Xi Jinping concordaron que el uso de armas nucleares no debe estar bajo el control de la IA. Notigram.

https://notigram.com/internacional/en-el-mundo/joe-biden-y-xi-jinping-concordaron-que-el-uso-de-armas-nucleares-no-debe-estar-bajo-el-control-de-la-ia-20241116-1366479

OpenAI. (2025, enero 30). Strengthening America's AI leadership with the U.S. National Laboratories. OpenAI. https://openai.com/index/strengthening-americas-ai-leadership-with-the-us-national-laboratories/

Organismo Internacional de Energía Atómica (OIEA). (s.f.). El OIEA y el Tratado sobre la No Proliferación. https://www.iaea.org/es/temas/el-oiea-y-el-tratado-sobre-la-no-proliferacion

Real Instituto Elcano. (s.f.). El nuevo tratado START: algo más que una limitación a las armas nucleares (ARI). https://www.realinstitutoelcano.org/analisis/el-nuevo-tratado-start-algo-mas-que-una-limitacion-a-las-armas-nucleares-ari/

Redacción HuffPost. (2025, enero 3). Rusia forja una alianza con el país de las armas futuristas para lanzar un desafío a EEUU. El HuffPost. https://www.huffingtonpost.es/global/rusia-forja-alianza-pais-armas-futuristas-lanzar-desafio eeuu.html

Sankaran, J. (2019). A different use for artificial intelligence in nuclear weapons command and control. War on the Rocks. https://warontherocks.com/2019/04/a-different-use-for-artificial-intelligence-in-nuclear-weapons-command-and-control/

Tiempo. (s.f.). La loca historia del incidente de 1983 que pudo causar un apocalipsis nuclear. https://www.tiempo.com/noticias/ciencia/la-loca-historia-del-incidente-1983-que-pudo-causar-apocalipsis-nuclear.htm