**DISEC**

*Comisión de Desarme de las Naciones Unidas*

**MSMUN 2023**

***Mesa***

Andrea Arrubla

Susana David

**Lenguaje Oficial**

Español

**Tema**

Medidas para evitar la adquisición de armas de destrucción masiva por parte de grupos terroristas.

Ciberseguridad y armas cibernéticas.

***Tabla de contenidos***

**1.** Carta de bienvenida

**2.** Información general

**2.1** Historia del comité

**2.2** Objetivos del comité

**3. Tema A:** Medidas para evitar la adquisición de armas de destrucción masiva por parte de grupos terrorista

3.1. Marco teórico

3.2. Contexto histórico

3.3. Situación actual

3.4. Resoluciones previas

3.5. Respuesta internacional

3.6. Links de apoyo

3.7. Expectativas para el debate

**4. Tema B:** Ciberseguridad y armas cibernéticas.

 4.1. Marco teórico

4.2. Contexto histórico

4.3. Situación actual

4.4. Resoluciones previas

4.5. Respuesta internacional

4.6. Links de apoyo

4.7. Expectativas para el debate

**5.** **Delegaciones presentes en el comité**

**6. QARMAS**

 6.1. Tema A

 6.2. Tema B

**7. Referencias**

**1. Carta de bienvenida**

Estimados delegados,

Bienvenidas a MSMUN 2024. Es un honor para nosotras, Susana David y Andrea Arrubla, poder ser sus presidentas en esta versión de la Comisión de Desarme de las Naciones Unidas. Ambas, estamos encantadas de tenerlos en nuestro comité, ver su desarrollo y poder ayudarlos en lo que necesiten. En el modelo externo, los temas a tratar serán: “Medidas para evitar la adquisición de armas de destrucción masiva por parte de grupos terroristas” y “Ciberseguridad y armas cibernéticas”. Siendo estos dos unos temas de suma importancia ya que representan una amenaza para la seguridad nacional e internacional. Esperamos que cada uno de ustedes aporte al debate, no tenga miedo a participar y brinde sus mejores argumentos y soluciones. De antemano, esperamos mucha preparación y durante las sesiones una buena disposición y contribución, pudiendo así tener un debate ordenado y claro.

 Como sus presidentas, cuentan con nosotras en cualquier momento o situación que se les presente. No duden en contactarnos si tienen alguna duda o si necesitan alguna ayuda o aclaración. Estaremos ahí para lo que necesiten, puesto que el objetivo es que mejoren cada vez más como delegados y líderes del futuro. Para finalizar, las invitamos a que den lo mejor de cada una, piensen de maneras diferentes a lo convencional, disfruten el proceso y aprovechen todo lo que aprenderán con este modelo. Sabemos que estas oportunidades son imprescindibles para el desarrollo de cada una como ser académico y ser humano. No lo olviden, en MSMUN hacemos lo imposible *posible.*

Cordialmente,

Presidente David Presidente Arrubla

 +57 3022519599 +57 300 3949694 susanadavidjimenezpp@gmail.com andrea.arrublaarroyave@gmail.com

 **2. Información general**

**2.1. Historia del comité**

La Comisión de Desarme y Seguridad Internacional (DISEC) es uno de los órganos principales de la Organización de las Naciones Unidas (ONU) encargado de la regulación de armas y la promoción de la paz mundial. Esta comisión fue creada en 1946, después de la Segunda Guerra Mundial, con el propósito de abordar la creciente preocupación mundial sobre la carrera armamentista y el peligro que representaba la amenaza nuclear. En sus inicios, la Comisión de Desarme estuvo bajo la jurisdicción del Consejo de Seguridad de la ONU, pero en 1978, durante las primeras sesiones de la Asamblea General, se convirtió en un órgano subsidiario de la Asamblea General.

Desde entonces, la Comisión ha trabajado en diversos temas relacionados con el desarme, incluyendo armas nucleares, armas químicas, armas biológicas, armas convencionales y municiones. Con el pasar de los años, la DISEC ha realizado importantes recomendaciones a los Estados Miembros de la ONU en materia de desarme y seguridad internacional. Estas han sido esenciales para la creación de tratados internacionales y acuerdos multilaterales con el fin de reducir el número de armas en circulación y fomentar la cooperación internacional en temas de seguridad. Una de las principales contribuciones de la DISEC fue el *Tratado de No Proliferación Nuclear* (TNP), firmado en 1968. El TNP se convirtió en uno de los principales acuerdos internacionales para evitar la propagación de armas nucleares y fomentar el uso pacífico de la energía nuclear.

 Seguidamente, la Comisión ha seguido trabajando en temas relacionados con el control y la regulación de armas nucleares. Y hacia el año de 1989, se tomó la decisión de establecer un número máximo de cuatro temas por año para que la Comisión pudiera ser más eficiente en su trabajo. En la práctica, en 1993, la Comisión se concentró en tan solo tres temas, y desde 2000 se ha limitado a tan sólo dos temas anuales. Esto ha permitido que la Comisión se enfoque en los temas más importantes y que pueda brindar soluciones eficaces a los problemas mundiales relacionados con el desarme y la seguridad internacional. Es importante destacar que la Comisión de Desarme y Seguridad Internacional no tiene la capacidad de movilizar tropas ni de iniciar guerras, sin embargo, su trabajo es esencial para garantizar la seguridad mundial, promover la paz y fomentar la cooperación internacional. En conclusión, la DISEC es un órgano clave de la ONU que sigue desempeñando un papel fundamental en la búsqueda de soluciones para los desafíos globales relacionados con el desarme y la seguridad.

 **2.2. Objetivos del comité**

 El principal objetivo de la Comisión de Desarme de las Naciones Unidas es mantener la seguridad internacional. Siendo la primera comisión de la asamblea general, se encarga del desarme mundial, y globalmente de la no proliferación de . Aunque la comisión interviene en cuestiones de seguridad internacional, no puede exigir o imponer acciones o sanciones gubernamentales o individuales para una intervención armada. Sin embargo, puede recomendar dichas acciones o sanciones a la asamblea general y luego al Consejo de Seguridad para que este las implemente. Concretamente, algunos de los temas tratados en dicha comisión son:

* Armas convencionales: Estas son todas las armas que no pueden clasificarse como armas de destrucción masiva. Son las más conocidas y utilizadas en entornos de conflicto y delincuencia y tienen una amplia gama de aplicaciones y un gran poder destructivo. El problema de estas armas es su regulación ya que las Naciones Unidas no prohíbe a sus estados miembros su eso DISEC busca regular estas para evitar que su tráfico ilícito caiga en manos de grupos criminales.
* Armas de destrucción masiva: Estas son aquellas que son capaces de eliminar grandes cantidades de personas de manera indiscriminada y a su vez causar daños económicos y ambientales. Dentro de estas se encuentran las armas químicas, nucleares y biológicas según dejan “cortinas radioactivas que se traducen en secuelas mortales en los sobrevivientes”. (IB, 2023) Específicamente, las armas químicas y biológicas afectan directamente la salud de cualquier ser vivo por sus efectos secundarios.
* Seguridad Internacional: Uno de los objetivos principales de la comisión es la paz y la seguridad internacional. Estas metas se alcanzarán por medio del desarme, la prevención de armas de destrucción masiva y el uso adecuado de las armas convencionales. De nuevo, DISEC no puede intervenir directamente en conflictos; cualquiera de sus resoluciones debe pasar por la asamblea general.

**3. Tema A: Medidas para evitar la adquisición de armas de destrucción masiva por parte de grupos terroristas.**

**3.1. Marco Teórico**

1. Armas nucleares:

“Un arma nuclear es un dispositivo que utiliza una reacción nuclear para crear una explosión. Esta explosión es mucho más potente que una con explosivos convencionales. Las armas nucleares pueden ser bombas o misiles.” (CDC, 2022)

1. Armas biológicas:

“El uso de microorganismos (virus, bacterias) o agentes bioactivos (toxinas), con el fin de producir enfermedades a las fuerzas militares enemigas, a la población civil o contaminar sus fuentes de agua o alimentación, es lo que conocemos como guerra biológica.” (Torrades, 2002).

1. Armas químicas:

“Un arma química es una sustancia química que se utiliza para causar intencionalmente daños o la muerte por medio de sus propiedades tóxicas.” (OPAQ, 2023)

1. Arsenales:

“Depósito o almacén general de armas y otros efectos de guerra.” (RAE, 2023)

1. Desarme:

“Arbitrio diplomático para mantener la paz, mediante la voluntaria reducción, equitativamente proporcional, de sus respectivas fuerzas militares, pactada por número suficiente de naciones.” (RAE, 2023)

1. Terrorismo:

“Actuación criminal de bandas organizadas, que, reiteradamente y por lo común de modo indiscriminado, pretende crear alarma social con fines políticos.” (RAE,2022)

1. Terrorismo químico, biológico, radiológico y nuclear (QBRN): acrónimo que proviene de la abreviación en inglés de Chemical, Biological, Radiological, and Nuclear (CBRN). Se utiliza para referirse a armas o materiales peligrosos que pertenecen a estas categorías.

**3.2 Contexto histórico**

*“La posibilidad de que agentes no estatales, incluidos los grupos terroristas y sus partidarios, tengan acceso a armas y materiales de destrucción masiva y los utilicen es una grave amenaza para la paz y la seguridad internacional.”*

* Vladimir Voronkov, Secretario General Adjunto de la Oficina de Lucha Contra el Terrorismo de las Naciones Unidas.

Las armas de destrucción masiva han tenido un gran impacto en la evolución del ser humano. Dentro de estas se incluyen la nucleares, biológicas, químicas y radiactivas (King, 2022). Por más de que a simple vista pareciera que aquellas son de origen reciente, a cualquiera sorprendería saber que han sido usadas en siglos anteriores. Los inicios de cada una de estas han variado a través de la historia. En primer lugar, las armas nucleares tuvieron su aparición el 6 de agosto de 1945, cuando los Estados Unidos de América hizo la prueba conocida como “Trinity” en Nuevo México explotando la primera bomba nuclear, hoy en día conocida como la bomba atómica. Exactamente tres días después de la exitosa detonación, la misma bomba fue lanzada sobre las ciudades de Hiroshima y Nagasaki en Japón dejando más de 200.000 afectados. Un año después, la Unión Soviética, compitiendo con los Estados Unidos decidió también empezar a construir sus propias armas nucleares, lo que desató la Guerra Fría dividiendo el mundo en dos bloques. Desde entonces se han creado varias armas nucleares y se han hecho varias pruebas, entre estas el “First Lightning” que fue la primera arma nuclear creada por la Unión Soviética y la “Bomba del Zar” una de las armas nucleares de más impacto a nivel internacional. En segundo lugar, las armas biológicas también han sido utilizadas a lo largo del tiempo de manera mucho más discreta que las nucleares. Los antepasados afirman que la mejor forma de atacar al opositor es causando una “enfermedad natural” y por lo tanto durante la antigua Roma las fuentes de agua potable que abastecen las ciudades eran envenenadas con enfermedades como el cólera, peste o lepra, con la finalidad de provocar enfermedades a la población civil adversaria. Durante la Segunda Guerra Mundial, se conoce del arma biológica utilizada por Japón contra la República Popular China, la cual consiste en esparcir pulgas infectadas con la peste bubónica en la ciudad de Changde. Asimismo, durante la Guerra Fría, la Unión Soviética se encargó de utilizar armas existentes como el ántrax y la viruela. Desde entonces el bioterrorismo es considerado uno de los más peligrosos pues cualquier microorganismo o patógeno genéticamente modificado puede causar la muerte de miles de personas y aumentar el bioterrorismo. En tercer lugar, las armas químicas, durante la Edad Media y el Renacimiento eran aquellas sustancias químicas en ámbitos militares para crear trampas como el humo tóxico, los proyectiles y flechas envenenadas, todas estas con la intención de atacar. Fue durante la Primera Guerra Mundial, que las armas químicas modernas empezaron a ser utilizadas, como por ejemplo los gases venenosos tales como el cloro, fosgeno y el gas mostaza generando primeramente daños en los tejidos y en el sistema respiratorio del bando opuesto. La guerra civil Española, Siria, y la guerra entre Irán e Irak también presentaron varios usos de aquellas armas de destrucción masiva específicamente del gas sarín y cloro. Después de ver las graves consecuencias sociales y ambientales de dichas armas de destrucción masiva, varias convenciones han ocurrido con enfoques específicos. Para las armas nucleares, se creó el TNP que significa [Tratado sobre la No Proliferación de las Armas Nucleares](https://www.iaea.org/sites/default/files/publications/documents/infcircs/1970/infcirc140_sp.pdf), este tiene que ser revisado cada 5 años. La última revisión fue en el año 2020, aquel tratado es un tratado internacional clave cuyo objetivo es prevenir la propagación de las armas nucleares y la tecnología armamentística, promover la cooperación en la utilización de la energía nuclear con fines pacíficos e impulsar el objetivo de lograr el desarme nuclear y el desarme general y completo. El TNP es el único tratado multilateral que representa un compromiso vinculante para los Estados poseedores de armas nucleares respecto del objetivo del desarme (Naciones Unidas, 2020). En cuanto a las armas biológicas, han ocurrido seis conferencias en torno a la prohibición de dichas armas, la última tomó lugar el 7 de enero de 2006. En aquel tratado multilateral se acordó que todos los estados pertenecientes a él están obligados a dar datos sobre laboratorios y centros de investigación; información sobre instalaciones de producción de vacunas; información sobre programas nacionales de investigación y desarrollo en materia de defensa contra las armas biológicas; declaración de actividades pasadas en el marco de programas de investigación y desarrollo biológico con fines ofensivos y/o defensivos; información sobre brotes epidémicos de enfermedades infecciosas e incidencias similares causadas por toxinas; publicación de resultados y promoción del empleo de conocimientos y contactos; información sobre legislación, reglamentaciones y otras medidas. De esta forma, las Naciones Unidas y los expertos estarán al tanto de cualquier riesgo que pueda terminar en un arma biológica. Por último y con base en las armas químicas, ocurrió la Convención sobre Armas Químicas (CAQ) en 1997. En esta, se prohíbe la producción, el almacenamiento y el uso de dichas armas y a su vez exige la destrucción de cualquier arsenal ya existente. En la CAQ se otorgó a la Organización para la Prohibición de las Armas Químicas (OPAQ), el poder de mandato para erradicar completamente el flagelo de las armas químicas y confirmar su destrucción dentro de los arsenales ya declarados. En la misma, se hicieron acuerdos de confidencialidad y participación activa de la industria química para garantizar que las empresas seguirán cooperando con el sistema de verificación industrial establecido por la CAQ.

**3.3. Situación actual**

Es más que evidente que en la actualidad hay varios grupos insurgentes causando múltiples repercusiones a nivel global. Cabe resaltar que el terrorismo es una amenaza para la vida humana, la política, economía y la más grande amenaza para la paz y la seguridad mundial. Existen varios medios por los cuales aquellos grupos terroristas se financian y adquieren todos los equipos para estar armados. En primer lugar, el mercado negro es una gran amenaza para la seguridad internacional, pues este facilita la compra ilegal de las armas de fuego actualmente bajo en su control, es decir que, si aquel contrabando continúa, el peligro constante de que algún arma de destrucción masiva caiga en manos de algún grupo insurgente podría llegar a ser posible causando repercusiones humanitarias y violaciones a los derechos humanos.



Figura 1. Tomado de Statista y el Instituto para la Economía y la Paz. (Ref.: 29).

De acuerdo con la Figura 1, los índices de terrorismo en el 2023 permanecen altos en varias regiones del mundo poniendo en alerta a los gobiernos y obligando a los organismos internacionales a abordar esta situación rápidamente. Según las estadísticas, varios países en el Medio Oriente se ven constantemente amenazados por varios grupos insurgentes que por medio del uso de armas de fuego o blancas amenazan a los civiles. Un claro ejemplo de aquellas amenazas a la seguridad y paz internacional se presenta en la nación de Libia. El tráfico de armas en naciones como esta impulsa el terrorismo de manera evidente no solo en el propio territorio, sino también en toda la región. Las armas procedentes de Libia han fortalecido enormemente la fuerza militar de los grupos terroristas que operan en muchas partes de la región, incluidos Argelia, Egipto, Malí y Túnez, entre otros. (Consejo de Seguridad). Así mismo, el contrabando ilegal por varios países en la región ha conseguido impulsar conflictos actuales como el de Israel- Palestina y el de Siria, dos de los conflictos que han perdurado por esta problemática y financiación del terrorismo y que podrían llegar a mayores si los terroristas llegan a tener acceso a armas de destrucción masiva.

La proliferación de armas de destrucción masiva (ADM) es uno de los obstáculos más grandes para la comunidad internacional. La mayoría de los países adhieren a tratados y acuerdos internacionales que prohíben o restringen su producción o posesión. Sin embargo, algunos países pueden participar en actividades no reveladas o encubiertas que impliquen armas de destrucción masiva. Según la Interpol, los atentados terroristas con materiales QBRNE (químicos, biológicos, radiactivos, nucleares y explosivos) podrían tener consecuencias catastróficas en la población y las infraestructuras. Algunos de los países que durante la historia se han mostrado con preocupación o han alzado sospechas de ser productores de ADM son Corea del Norte, Siria, Libia, Irán e Israel. Es necesario encontrar una solución, pues es evidente que aunque la ley obligue a naciones proliferantes a reportar, varias lo evaden.

**3.4. Resoluciones previas**

*Respuestas de la ONU*

* Oficina de lucha contra el terrorismo (UNOCT)

Esta organización dispone de un grupo de trabajo interinstitucional sobre Prevención y Respuesta a Atentados Terroristas con Armas de Destrucción Masiva, cuyo objetivo es mejorar la coordinación en la planificación de la respuesta ante un atentado terrorista con armas o materiales QBRN.

* Interpol

La policía internacional se ha encargado de ayudar estados miembros a evitar y estar capacitados en caso de algún ataque de ADM. Para poder ejecutar dicho plan de manera efectiva, la interpol recurre al intercambio de información, el análisis de inteligencia y la formación y apoyo operativo de las naciones.

* Consejo de Seguridad: En la resolución 1540 del 2004, el órgano con máximo poder de la ONU, decidió que todos los Estados deberían abstenerse de brindar apoyo a actores no estatales que traten de desarrollar, adquirir, fabricar, poseer, transportar, transferir o utilizar armas nucleares, químicas y biológicas y sus sistemas vectores, especialmente con fines terroristas. La resolución llama a todos los Estados a adoptar e implementar legislación efectiva al respecto, así como otras medidas efectivas para prevenir la proliferación de armas y sus sistemas vectores a actores no estatales, especialmente con fines terroristas. (Naciones Unidas, 2004)

**3.5. Respuesta internacional**

Con base en las armas de destrucción masiva (ADM) varias naciones han mostrado su posición con respecto a ellas, sin embargo, algunas siguen sin tener una posición clara. Con respecto a las armas nucleares, delegaciones tales como la de Estados Unidos, Francia, Reino Unido, China y Rusia cuentan con arsenales de armas nucleares y son conocidos como "Estados con armas nucleares reconocidos" y son signatarios del Tratado de no Proliferación de armas nucleares en virtud del Artículo IX del tratado. Por otro lado, delegaciones no firmantes del TNP como lo son la India, Pakistán y Corea del Norte han realizado experimentos con armas nucleares. Delegaciones como Israel nunca han admitido, pero tampoco han negado contar con armamento nuclear. Recientemente, el estado judío a estado produciendo armamento nuclear desde hace más de 50 años, llevándolo a ser considerado un estado o potencia nuclear. Israel es reconocido por ser el único país que cuenta con dichas armas en el medio oriente, aquello también se le ve como amenaza pues los terroristas de la región Palestina, Hamas, no están tan lejos de obtener aquellas ADM.

 La mayoría de las delegaciones presentes en el comité son naciones firmantes y participantes de la CAQ (Convención de Armas Químicas) en la cual se prohíbe el desarrollo, la producción, el almacenamiento y el uso de armas químicas. Sin embargo, recientemente se ha visto cómo estas han sido utilizadas en conflictos dentro de las naciones como Siria y Líbano. En tales delegaciones no solo han habido acusaciones del uso de armas químicas de parte del gobierno contra los civiles, sino que también varios grupos terroristas han sido reconocidos usándolas. La comunidad internacional está al tanto de las guerras internas de estas naciones, sin embargo, no hay acción.

En cuanto a las armas biológicas, la Convención para la prohibición de las Armas Biológicas (CABT), prohíbe su desarrollo, su producción y su almacenamiento y su uso en tiempos de guerra. Algunos de los países firmantes de dicha convención, que aún hoy en día se supone que siguen aquellos requisitos son: Estados Unidos, Rusia, China, Francia, Reino Unido, Alemania, Canadá, Japón, India y Brasil. En cambio, aquellos países que se rehúsan ser signatarios en dicha convención son por ejemplo Corea del Norte y Sudán del Sur.

**3.6. Links de apoyo**

* ACNUR. (2004, Diciembre 16). Medidas para evitar la adquisición por terroristas de armas de destrucción en masa. Naciones Unidas. <https://www.acnur.org/fileadmin/Documentos/BDL/2005/3462.pdf>
* Unidos contra el terrorismo. (n.d.). *Unidos contra el terrorismo.* [https://www.un.org/spanish/unitingagainstterrorism/dificultar.htm](https://www.un.org/spanish/unitingagainstterrorism/dificultar.html)l
* Naciones Unidas. (s.f.). Desarme.

<https://www.un.org/es/global-issues/disarmament>

* Naciones Unidas y terrorismo. (s.f.) Ministerio de Europa y asuntos extranjeros. <https://www.diplomatie.gouv.fr/es/politica-exterior/seguridad-desarme-y-no-proliferacion/terrorismo-accion-internacional-de-francia/naciones-unidas-y-terrorismo/>
* Adell, M. (2019, Octubre 9). *ARMAS DE DESTRUCCIÓN MASIVA Y TERRORISMO. El control de las exportaciones en el marco de la Resolución 1540 (2004).* Observatorio Internacional de estudios sobre el terrorismo. <https://observatorioterrorismo.com/actividades/armas-de-destruccion-masiva-y-terrorismo-el-control-de-las-exportaciones-en-el-marco-de-la-resolucion-1540-2004/>
* Comité Internacional de la Cruz Roja. (1999, Junio 6). *Esfuerzos para limitar y controlar la disponibilidad de armas.* CICR. <https://www.icrc.org/es/doc/resources/documents/misc/5tdnee.html>

**3.7. Expectativas para el debate**

De antemano, gracias por elegir el comité DISEC, contamos con que en estas sesiones den lo mejor de ustedes. En primer lugar, esperamos de ustedes mucho compromiso, orden y puntualidad al entregar los papeles de posición con los preámbulos y fechas asignadas, así podremos estar seguros de su comprensión del tema y que serán una buena representación para su delegación. En segundo lugar, esperamos que prevalezca el valor del respeto y la objetividad a la hora de los debates, sabemos que este es un tema complicado y que habrá diferentes perspectivas y opiniones. Les pedimos que toquen todos los aspectos mencionados en esta específica sección de la guía, desde los distintos accesos a armas de destrucción masiva por parte de los grupos insurgentes, hasta los ataques y consecuencias a corto y largo plazo de estos. Es importante que se encarguen de incluir los tres tipos de armas de destrucción masiva mencionados en la guía, pues el fin del comité es encontrar medidas para evitar su uso por terroristas. Así mismo, les pedimos que se enfoquen en tratar de encontrar una solución específicamente para aquellos dos obstáculos presentados en la situación actual. Propongan soluciones y no tengan miedo pues nadie los estará juzgando, solo apoyando. Busquen nuevas alternativas y sean originales. Por último, esperamos de ustedes nada más y nada menos que un rendimiento excelente y que no duden en buscarnos porque estamos para ayudarles en lo que necesiten.

**4. Tema B: Ciberseguridad y armas cibernéticas**

**4.1. Marco Teórico**

1. Ataques de denegación de servicio (DDoS): “Implica inundar un sitio web con solicitudes falsas, lo que obliga al sitio a procesar esas solicitudes, dejándolo sin funcionamiento para usuarios legítimos. Este tipo de ataque podría usarse para paralizar un sitio web crítico utilizado por ciudadanos, personal militar, personal de seguridad, científicos u otros para interrumpir operaciones o sistemas críticos”. (Torres, 2022)
2. Ataques a infraestructura crítica:

“Hackear la red de energía eléctrica podría dar a un atacante la capacidad de desactivar sistemas críticos, paralizar la infraestructura y causar daños severos. Además, un ataque a la red eléctrica podría interrumpir las comunicaciones, imposibilitando el uso de servicios como la mensajería de texto o las telecomunicaciones”. (Torres, 2022)

1. Ciberespacio:

Ámbito virtual creado por medios informáticos. (RAE, 2023)

1. Espionaje: Se refiere a espiar a otro país para robar secretos. En la guerra cibernética, esto puede implicar el uso de una red de bots o un ataque de pesca submarina para afianzarse en una computadora antes de extraer información confidencial. Aunque el espionaje tradicional y el ciber espionaje no se consideran actos de guerra por sí mismos, a menudo se definen como ataques en el contexto de la ciberguerra. Una parte significativa de los ataques informáticos en este escenario se basa en actividades de espionaje. (LISA institute, 2022)
2. Hacker: Experto en informática, capaz de acceder a un sistema sin autorización, normalmente para detectar sus fallos de seguridad y desarrollar mejoras. (RAE, 2023)
3. Interrupción Económica Los ciberataques en una ciberguerra a menudo causan daños al tejido financiero, afectando empresas, ciudadanos y, finalmente, la economía del país enemigo. Grandes empresas, bancos y bolsas de valores son objetivos primarios para los hackers respaldados por gobiernos, afectando gravemente la estabilidad económica. (LISA institute, 2022)
4. Ransomware: Utilizado para secuestrar datos y obtener dinero, pero también puede tener fines destructivos. Ejemplos notables incluyen el ataque NotPetya en 2017, atribuido a Rusia, que afectó a nivel mundial. (LISA institute, 2022)
5. Phishing: La palabra phishing quiere decir suplantación de identidad. Es una técnica de ingeniería social que usan los ciberdelincuentes para obtener información confidencial de los usuarios de forma fraudulenta y así apropiarse de la identidad de esas personas.(Argentina GOB, 2023)
6. Propaganda: En la ciberguerra, la propaganda implica controlar la información para influir en la opinión pública. Se realiza a través de ataques de desinformación en redes sociales y medios digitales, así como la difusión de noticias falsas. Este tipo de guerra psicológica busca manipular opiniones y comportamientos, siendo también utilizado por organizaciones terroristas para reclutar miembros. (LISA institute, 2022)
7. Sabotaje: Los equipos informáticos, satélites y centros de suministro, transporte y comunicaciones son objetivos comunes en una ciberguerra. Estos ataques buscan interrumpir servicios o causar daños sustanciales. Los sistemas informáticos pueden ser interceptados y reemplazados por otros maliciosos. (LISA institute, 2022)

**4.2 Contexto histórico**

Desde el origen de los tiempos, el ser humano ha combatido con las armas y con la tecnología esto no fue la excepción. De esta forma, el ciberespacio ha pasado a convertirse en un entorno más. El objetivo de las fuerzas especializadas en el combate en el ciberespacio persigue el mismo objetivo que en el resto de los ámbitos: garantizar la libertad de acción de las fuerzas propias y negársela al adversario. De esta forma, podemos entender la ciberguerra como el conflicto armado que se desarrolla fundamentalmente en o a través del ciberespacio. La ciberguerra, o guerra tecnológica, ha evolucionado como una forma de conflicto en la era digital, aprovechando la interconexión global a través de internet. A medida que la tecnología avanzó, los países comenzaron a utilizar ataques digitales para comprometer los sistemas informáticos esenciales de otros estados. Este fenómeno se ha convertido en una herramienta estratégica en las relaciones internacionales, con el propósito de encontrar vulnerabilidades y causar daño en infraestructuras críticas. Esta se ejecuta principalmente a través de hackers respaldados por estados, quienes emplean virus informáticos, ataques de piratería, infiltración en redes enemigas, recopilación de datos, interferencia de señales inalámbricas y otros métodos. A medida que la tecnología avanza, las tácticas de combate en la ciberguerra evolucionan, incluyendo el uso de armas como ransomware y ataques DDoS.

Las principales potencias en este campo incluyen a Estados Unidos, China y Rusia, junto con otros países destacados como Israel, Francia, Taiwán, Irán y otros. La ciberguerra ha demostrado ser un medio efectivo para la obtención de información sensible, la interrupción de servicios esenciales y el daño económico.

En cuanto a los tipos de ciberguerras, estas pueden involucrar desde espionaje y sabotaje hasta propaganda y ataques para interrumpir la economía del enemigo. Los actores no estatales también desempeñan un papel crucial en este escenario, lo que agrega complejidad a la situación geopolítica.

Algunos ejemplos de ciberguerras que han ocurrido durante los últimos años son:

Ciberataque ruso en Ucrania en 2017: En esta guerra se hizo uso de un ransomware diseñado para destruir datos. EEUU y Reino Unido culparon a Rusia de la creación del ransomware NotPetya, que llegó a considerarse el “ciberataque más destructivo y costoso de la historia” hasta ese momento. Aunque este ciberataque, probablemente, sólo tuviera como objetivo Ucrania, se extendió rápidamente, causando daños en muchos países que costaron miles de millones de dólares.

Uso de noticias falsas en elecciones: En México, en 2018, se descubrió una red de noticias falsas cuya pretensión era interferir en las elecciones presidenciales. Ese mismo año, el Ministerio de Defensa de España denunció un ciberataque a su red por parte de una “potencia extranjera”.

Ataques entre China, Estados Unidos y Rusia: China es uno de los países que más sufren ataques cibernéticos. Un informe realizado en el país en junio de 2018 afirma que la mayor parte de los ciberataques que sufre el país provienen de EEUU (LISA institute). Por otra parte, un artículo de *The New York Times* afirmó que el Pentágono y los servicios de Inteligencia de EEUU estaban llevando a cabo ciberataques masivos contra las redes de suministro eléctrico en Rusia. Durante el año 2019, las grandes potencias mundiales intercambiaron acusaciones de ciberataques y espionaje. EEUU considera que las mayores amenazas en el marco de una ciberguerra son China y Rusia. Piratas cibernéticos (Hackers) respaldados por China también han intentado obtener información secreta de los proveedores de servicios de tecnología extranjeros. Asimismo, parece probable que EEUU esté utilizando ataques cibernéticos contra el ISIS como parte de una ciberguerra.

 **4.3. Situación actual**

En la actualidad, la ciberguerra se ha convertido en una preocupación crucial en las relaciones internacionales. La guerra híbrida se ha vuelto más prominente, extendiéndose más allá de los medios tradicionales y utilizando internet como el principal campo de batalla. Los conflictos híbridos, combinan el uso de la fuerza militar con otros elementos como pueden ser los ciberataques, la manipulación de la información a través de internet y de las redes sociales. Las principales potencias en la ciberguerra, como Estados Unidos, China y Rusia, junto con otros países destacados, compiten por la supremacía digital. La falta de normas internacionales específicas que regulen estos conflictos, plantea desafíos para la seguridad global.

Ciberseguridad:

La ciberseguridad se ha convertido en una prioridad crítica en la actualidad, ya que los ciberataques pueden afectar a cualquier infraestructura, desde sectores financieros y políticos hasta la salud y la vida cotidiana. La interconexión global ha hecho que los países sean vulnerables a ciber amenazas difusas y desconocidas. Los esfuerzos para defenderse contra la ciberguerra incluyen estrategias de ciberseguridad a nivel individual, empresarial y estatal. Cambiar contraseñas, utilizar medidas de protección avanzadas y actualizar sistemas son prácticas comunes. Sin embargo, la ciberguerra también plantea la necesidad de establecer límites internacionales y regulaciones claras para abordar este desafío. La ciberseguridad es más importante que nunca. Los ciberataques, pueden afectar a cualquier infraestructura financiera, política, empresarial e incluso de salud.

Las armas cibernéticas varían desde métodos relativamente simples, como correos electrónicos de phishing, hasta tácticas altamente sofisticadas. La preocupación radica en que estas armas pueden ser analizadas y mejoradas por los países afectados, lo que lleva a una escalada en la ciberguerra. La propagación de armas cibernéticas y la participación de actores no estatales subrayan la gravedad de la ciberguerra y la necesidad urgente de fortalecer la ciberseguridad a nivel global.

  **4.4. Resoluciones previas**

A pesar de que la ciberguerra es una situación relativamente reciente y aún no se han hecho tratados o soluciones “concretas”, existe una creciente inquietud por parte de la ONU acerca del uso indebido de la tecnología de la información y de las comunicaciones por parte de terroristas, especialmente a través de Internet y las nuevas tecnologías digitales. Los Estados Miembros han subrayado la importancia de la cooperación entre diversas partes involucradas para abordar esta amenaza, incluyendo también a organizaciones internacionales, regionales y subregionales, el sector privado y la sociedad civil.

* Resolución 2341 (2017): El Consejo de Seguridad insta a los Estados Miembros a "establecer o fortalecer alianzas a nivel nacional, regional e internacional con las partes interesadas, tanto del ámbito público como privado, según corresponda, con el fin de intercambiar información y experiencias para prevenir, proteger, mitigar e investigar los daños causados por actos terroristas contra instalaciones críticas de infraestructura. También se destaca la necesidad de responder y recuperarse de tales ataques, especialmente a través de actividades conjuntas de capacitación y la utilización o creación de redes de alerta de emergencia o comunicación pertinentes".

La Oficina de las Naciones Unidas de Lucha Contra el Terrorismo (OLCT) tiene varias iniciativas en el ámbito de las nuevas tecnologías, incluido un proyecto sobre el uso de las redes sociales para reunir información de fuentes abiertas y pruebas digitales a fin de combatir el terrorismo y el extremismo violento respetando los derechos humanos. También brinda conocimientos especializados en foros internacionales acerca de los usos de los sistemas aéreos no tripulados y programará más actividades en este ámbito. Entre estos:

El Programa de Ciberseguridad y Nuevas Tecnologías: En este programa se fomenta las capacidades de los Estados Miembros y las organizaciones privadas en la prevención de ciberataques realizados por actores terroristas contra infraestructuras críticas. El proyecto también busca mitigar los efectos de los ataques y recuperar y restaurar los sistemas que sean el blanco de estos, si llegasen a ocurrir.

**4.5 Respuesta internacional**

En primer lugar, como una de las potencias líderes en ciberseguridad y tecnología, Estados Unidos reconoce la importancia de la ciberguerra. Ha expresado preocupaciones sobre ciberataques provenientes principalmente de China, Rusia, y Corea del Norte. Estados Unidos ha desarrollado capacidades ofensivas y defensivas en ciberseguridad y ha adoptado una postura agresiva para proteger sus intereses. (VOA, 2017)

Por otro lado, China es un actor importante en la ciberguerra, a menudo acusada de realizar ciber espionaje y ataques cibernéticos contra otros países, especialmente Estados Unidos. China ha negado estas acusaciones y sostiene que también es víctima de ciberataques. La ciberguerra puede ser vista como una extensión de la competencia geopolítica entre China y otras potencias. (Mancera, 2014)

Los países europeos, en general, reconocen la importancia de la ciberguerra y han tomado medidas para fortalecer sus capacidades de ciberseguridad. La Unión Europea ha buscado establecer normas y regulaciones para mitigar las amenazas cibernéticas y mejorar la cooperación entre los Estados miembros. (DW, 2022)

Sin embargo hay países tales como Corea del Norte, los cuales han sido asociados con actividades cibernéticas maliciosas, incluyendo ataques a sistemas informáticos y ciber espionaje. La ciberguerra puede ser vista como una herramienta para Corea del Norte en su búsqueda de influencia y seguridad nacional. (NYT, 2017)

Finalmente, Rusia e Israel son conocidos por su participación en operaciones cibernéticas. A Rusia se le ha acusado de interferir en elecciones y llevar a cabo ciberataques contra otros países. La ciberguerra es considerada como una herramienta para avanzar en los objetivos geopolíticos y desestabilizar a otras naciones. Sin embargo, Israel ve la ciberguerra como una amenaza significativa y ha desarrollado capacidades avanzadas para defenderse y llevar a cabo operaciones en este espacio. (LISA institute, 2022)

**4.6 Links de apoyo**

* *¿Qué es la ciberguerra?*

[*https://www.nationalgeographic.es/video/tv/que-es-la-ciberguerra*](https://www.nationalgeographic.es/video/tv/que-es-la-ciberguerra)

* *Ciberataques*

[*https://www.eitb.eus/es/tag/ciberataques/*](https://www.eitb.eus/es/tag/ciberataques/)

* *EEUU lanza agresiva estrategia nacional de ciberseguridad* [*https://www.vozdeamerica.com/a/eeuu-lanza-agresiva-estrategia-nacional-de-ciberseguridad/6986388.html*](https://www.vozdeamerica.com/a/eeuu-lanza-agresiva-estrategia-nacional-de-ciberseguridad/6986388.html)
* *Europa prepara su sistema de defensa para la ciberguerra*

*https://www.dw.com/es/europa-prepara-su-sistema-de-defensa-para-la-ciberguerra/a-63732312*

* *Ciberguerra: China y Corea del Norte mejoran sus capacidades de influencia*

[*https://www.channelpartner.es/seguridad/ciberguerra-china-y-corea-del-norte-mejoran-sus-capacidades-de-influencia/*](https://www.channelpartner.es/seguridad/ciberguerra-china-y-corea-del-norte-mejoran-sus-capacidades-de-influencia/)

* *El secretario general de la ONU dice que hay “ciberguerra entre Estados”*

[*https://elpais.com/internacional/2018/02/19/actualidad/1519058033\_483850.html*](https://elpais.com/internacional/2018/02/19/actualidad/1519058033_483850.html)

* *Un año de ciberataques tan increíbles como ciertos*

[*https://www.elespanol.com/invertia/disruptores-innovadores/opinion/20240114/ano-ciberataques-increibles-ciertos/824547546\_13.html*](https://www.elespanol.com/invertia/disruptores-innovadores/opinion/20240114/ano-ciberataques-increibles-ciertos/824547546_13.html)

**4.7 Expectativas para el debate**

En este segundo tema, no está de más decirles que también esperamos que prevalezca mucho respeto y objetividad. Sabemos que este es un tema relativamente reciente y que se puede dificultar un poco encontrar fuentes confiables y con información sobre cada una de sus delegaciones. Sin embargo sabemos que con diferentes fuentes académicas y con ayuda de la guía lograran preparase de manera correcta para el debate. Les pedimos que mencionen durante el debate todos los aspectos mencionados en la guía, los diferentes tipos de armas cibernéticas, el ataque cibernético de Rusia hacia Ucrania, las diferentes ocasiones en las cuales los ciberataques han afectado la seguridad internacional de muchas delegaciones y la resolución previamente establecida por la ONU para evitar este tipo de ataques. Es importante que traten de buscar soluciones a esta problemática mediante la cooperación de las diferentes naciones. Busquen nuevas alternativas, ya que en este tema se puede ser muy creativo y original, al no haber tantas resoluciones previamente establecidas. Por último, esperamos que se preparen bastante, pero sobre todo que disfruten cada argumento que hagan, que debatan mucho y que nos impresionen con sus habilidades, y por último que aprendan mucho durante todo el modelo.

**5. Delegaciones presentes en el comité**

* Estados Unidos
* Rusia
* China
* Francia
* Reino Unido
* Irán
* Irak
* Israel
* Libia
* Siria
* Corea del Norte
* Ucrania
* Palestina
* Alemania
* Venezuela
* Japón
* España
* Pakistan
* Taiwan
* México
* India
* Canadá
* Brasil

**6. QARMAS**

**6.1 Tema A**

* ¿Cómo está ligada su delegación a las armas de destrucción masiva? ¿Está a favor o en contra de estas?
* ¿Su delegación ha producido o utilizado ADM en el pasado?
* ¿Su delegación ha propuesto o participado en soluciones previamente implementadas para mejorar la situación con respecto a estas armas?
* ¿Qué perspectiva tiene la delegación con respecto a fortalecer la capacidad nacional para prevenir acceso a terroristas a las ADM ?
* ¿Cómo piensa que su delegación puede aportar a promover la cooperación internacional en materia de seguridad para prevenir el terrorismo ?
* ¿Las ADM han afectado de alguna manera a su delegación?
* ¿Su delegación constantemente reporta cualquier posible arma biológica, química o nuclear a los organismos de las Naciones Unidas?
* ¿Su delegación cuenta con grupos terroristas que le impiden contribuir y garantizar la seguridad con respecto a este tipo de armas?

**6.2 Tema B**

* ¿Cómo está ligada su delegación a la ciberguerra ?
* ¿Ha hecho su delegación ataques cibernéticos hacia otras delegaciones?
* ¿Ha participado su delegación en la resolución preventiva de la ONU sobre ciberseguridad?
* ¿De qué formas se ha visto afectada su delegación en la ciberguerra?
* ¿Ha tenido su delegación conflictos cibernéticos internos ?
* ¿Qué tipo de armas cibernéticas han sido usadas por su delegación o en contra de esta?
* ¿Su delegación ha propuesto posibles soluciones sobre el tema? ¿Cuáles?
* ¿Hace su país parte de los países miembros de la resolución establecida por la ONU?

**7. Referencias**

1. UN General Assembly - First Committee - Disarmament and International Security. (s.f.). https://www.un.org/en/ga/first/index.shtml
2. *Armas de Destrucción Masiva y Rescate*. (s.f.) Instituto Badra. <https://institucionbadra.org/talleres/armas-de-destruccion-masiva-y-actuacion-prehospitalaria/>
3. Blakemore, E. (2020, July 21). *Las armas nucleares y sus consecuencias históricas*. National Geographic.

<https://www.nationalgeographicla.com/historia/2020/07/las-armas-nucleares-y-sus-consecuencias-historicas>

1. Castaño, J. M. (2014). *La ciberguerra china desde la lógica de la guerra irrestricta*. Dialnet. https://dialnet.unirioja.es/servlet/articulo?codigo=5682905
2. Centers for Disease Control and Prevention. (2022, Julio 5). *Radiation Emergencies - Radiation and your health.* <https://www.cdc.gov/nceh/radiation/emergencies/index.htm?CDC_AA_refVal=https%3A%2F%2Femergency.cdc.gov%2Fradiation%2Findex.asp>
3. Council of Europe. (s.f). *Guerra y Terrorismo.* https://www.coe.int/es/web/compass/war-and-terrorism
4. Cubeiro, E. (2019, June 9). *Ciberguerra: El conflicto armado que se desarrolla a través del ciberespacio*. Defensa.com.

<https://www.defensa.com/cyberseguridad/ciberguerra>

1. El Mundo. (s.f.).*Informe de Naciones Unidas: El tráfico de armas en Libia impulsa la am*enaza terrorista en la región. <https://www.elmundo.es/internacional/2015/03/02/54f42cdce2704ea5578b456d.html>
2. EEUU lanza una agresiva estrategia nacional de ciberseguridad. (2023, March 2). Voz de América. https://www.vozdeamerica.com/a/eeuu-lanza-agresiva-estrategia-nacional-de-ciberseguridad/6986388.html
3. Gobierno de España. (s.f.). *Convención para la prohibición de las Armas Biológicas: una herramienta para la seguridad internacional. Ministerio de asuntos exteriores y cooperación.* https://www.miteco.gob.es/content/dam/miteco/es/calidad-y-evaluacion-ambiental/temas/biotecnologia/Divulgacion%20CABT\_tcm30-190285.pdf
4. Gratacós, V. (2020, Octubre 25). Nucleares, biológicas y químicas: la lucha internacional contra las armas de destrucción masiva. El Orden Mundial. <https://elordenmundial.com/nucleares-biologicas-quimicas-internacional-armas-destruccion-masiva/>
5. INTERPOL. (s.f.). Terrorismo.

https://[www.interpol.int/es/Delitos/Terrorismo](http://www.interpol.int/es/Delitos/Terrorismo)

1. *Israel, potencia nuclear encubierta*. (2022, Septiembre 9). SwissInfo. https://www.swissinfo.ch/spa/irán-nuclear\_israel--potencia-nuclear-encubierta-y-bestia-negra-del-pacto-nuclear-con-irán/47911236
2. King, S. (2022, September). *Weapons of Mass Destruction.* ELSEVIER. <https://www.sciencedirect.com/science/article/abs/pii/S1553838922006066?via%3Dihub>
3. LISA institute. (n.d.). *Ciberguerra: tipos, armas, objetivos y ejemplos de la guerra tecnológica*. LISA Institute <https://www.lisainstitute.com/blogs/blog/ciberguerra-tipos-armas-objetivos-ejemplos>
4. LISA institute. (n.d.). *Qué es la Guerra Híbrida y cómo nos afectan las Amenazas Híbridas*. LISA Institute. https://www.lisainstitute.com/blogs/blog/guerra-hibrida-amenazas-hibridas?\_pos=1&\_sid=2a00a65a2&\_ss=r
5. Naciones Unidas. (s.f.) *Desarme.*

[https://www.un.org/es/global-issues/disarmament#:~:text=Entre%20las%20más%20conocidas%20armas,guerra%2C%20misiles%20y%20lanzamisiles%2C%20minas](https://www.un.org/es/global-issues/disarmament#:~:text=Entre%20las%20m%C3%A1s%20conocidas%20armas,guerra%2C%20misiles%20y%20lanzamisiles%2C%20minas)

1. Naciones Unidas. (s.f.). *Décima Conferencia de las Partes encargada del examen del Tratado sobre la No Proliferación de las Armas Nucleares.* <https://www.un.org/es/conferences/npt2020/background>
2. Naciones Unidas. (2004). *Resolución 1540 (2004) del Consejo de Seguridad de las Naciones Unidas.* Oficina de asuntos de desarme. https://disarmament.unoda.org/es/adm/resolucion-1540-2004-del-consejo-de-seguridad-de-las-naciones-unidas/
3. Noticias ONU. (2018, Abril 4). El uso de armas químicas en Siria no puede quedar impune. Naciones Unidas.

[https://news.un.org/e](https://news.un.org/es/story/2018/04/1430331)

1. Oficina de Asuntos de Desarme. (s.f.). La Convención sobre las Armas Biológicas. Naciones Unidas. [https://disarmament.unoda.org/es/adm/armas-biologicas/#:~:text=La%20Convención%20sobre%20las%20Armas%20Biológicas%2C%20el%20primer%20tratado%20multilateral,26%20de%20marzo%20de%201975](https://disarmament.unoda.org/es/adm/armas-biologicas/#:~:text=La%20Convenci%C3%B3n%20sobre%20las%20Armas%20Biol%C3%B3gicas%2C%20el%20primer%20tratado%20multilateral,26%20de%20marzo%20de%201975).
2. ¿Qué es el phishing? (n.d.). Argentina.gob.ar.

https://www.argentina.gob.ar/justicia/convosenlaweb/situaciones/phishing

1. RAE. (s.f) *Arsenal.*

<https://dle.rae.es/arsenal>

1. RAE. (s.f) Ciberespacio

[https://dle.rae.es/](https://dle.rae.es/terrorismo)ciberespacio

1. RAE. (s.f) Jáquer

[https://dle.rae.es/](https://dle.rae.es/terrorismo)jáquer

1. RAE. (s.f) Terrorismo.

<https://dle.rae.es/terrorismo>

1. Riegert, B. (2022, November 11). *Europa prepara su sistema de defensa para la ciberguerra – DW – 11/11/2022*. DW. <https://www.dw.com/es/europa-prepara-su-sistema-de-defensa-para-la-ciberguerra/a-63732312>
2. Perlroth, N. (2017, October 18). *El mundo ya no se burla del poderío cibernético de Corea del Norte (Published 2017)*. The New York Times. https://www.nytimes.com/es/2017/10/18/espanol/el-mundo-ya-no-se-burla-del-poderio-cibernetico-de-corea-del-norte.html
3. Statista. (2023, Marzo 15). *El impacto del terrorismo en el mundo.* Instituto para la Economía y la Paz. https://es.statista.com/grafico/26978/impacto-del-terrorismo-en-los-paises-segun-el-indice-global-de-terrorismo/
4. The New York Times. (1997, Febrero 4). *Japón experimentó la guerra biológica en China durante la II Guerra Mundial.* El País. https://elpais.com/diario/1997/02/05/internacional/855097210\_850215.html
5. Torrades, S. (2002, Abril). *La ingeniería genét*ica y el desarrollo de las armas biológicas. ELSEVIER. [https://www.elsevier.es/es-revista-offarm-4-articulo-la-ingenieria-genetica-el-desarrollo-13028953#:~:text=de%20otros%20continentes.-,Durante%20la%20Primera%20y%20la%20Segunda%20Guerra%20Mundial%20se%20realizaron,atacar%20a%20la%20población%20civil](https://www.elsevier.es/es-revista-offarm-4-articulo-la-ingenieria-genetica-el-desarrollo-13028953#:~:text=de%20otros%20continentes.-,Durante%20la%20Primera%20y%20la%20Segunda%20Guerra%20Mundial%20se%20realizaron,atacar%20a%20la%20poblaci%C3%B3n%20civil).
6. Torres, A. (2022, June 27). *Conceptos básicos sobre ciberguerra - Prensario Tila*. Prensario TI. <https://prensariotila.com/conceptos-basicos-sobre-ciberguerra/>
7. UN. (n.d.). Ciberseguridad | Oficina de Lucha contra el Terrorismo. https://www.un.org/counterterrorism/es/cybersecurity