LMUN 2026

Guía de antecedentes de la:

Organización del Tratado Atlántico del Norte

LMUN 2026

OTAN | De la Guerra Fría a la Guerra Digital: La OTAN Frente a los Ciberataques

Directora: Luciana Monge

Co-Directora: Lara Garita

Carta de Introducción

Queridos delegados,

Es un honor para nosotras darles la bienvenida al comité de la OTAN del LMUN 2026. Mi nombre es Luciana Monge y seré su directora de mesa junto a mi codirectora Lara Garita. Ambas tenemos 16 años y estamos actualmente cursando el 10.º año en el colegio Lincoln. Contamos con una sólida trayectoria en Modelos de Naciones Unidas, ya que desde 2023 llevamos atendiendo estas mismas.

Este será nuestro primer comité siendo Directora y Co-directora y no podríamos estar más emocionadas de crear un debate en el que cada uno de ustedes salga con amplio entendimiento del tema. Como equipo esperamos tener un debate dinámico en el que cada uno pueda representar a su delegación de la mejor manera. De igual manera trabajaremos para que esta sea una experiencia divertida y agradable para todos. Anticipamos con emoción la evolución de este comité, esperando que se logre llegar a un consenso que beneficie a cada una de las naciones presentes.

Si tienen alguna duda, comentario, o preocupación no duden en contactarnos. ¡Esperamos verlos pronto!

Lucia Monge Arrieta
lumonge@lincoln.ed.cr

Lara Garita Sauma
Lgarita@lincoln.ed.cr

Introducción al Tema

En un mundo cada vez más interconectado, el acelerado desarrollo tecnológico y la creciente dependencia del ciberespacio han transformado la manera en la que los Estados conciben la seguridad y la defensa. A diferencia de los conflictos tradicionales, los ciberataques no conocen fronteras físicas, y su impacto puede ser devastador; desde afectar severamente el financiamiento de bancos hasta sacar información privada de instituciones y servicios de comunicación. Es clave entender que el creciente uso de herramientas digitales ha abierto un nuevo escenario para el conflicto; a través de esto, los ciberataques se han convertido en una amenaza constante contra la seguridad nacional.

Como respuesta a este riego, varios países han implementado políticas como la estrategia de ciberseguridad de la OTAN, el Reglamento General de Protección de Datos (GDPR) de la Unión Europea y las Estrategias Nacionales de Ciberseguridad en Estados Unidos y Canadá, las cuales buscan fortalecer la protección de datos, mejorar la respuesta ante incidentes y aumentar la cooperación internacional. Estas regulaciones han permitido una mayor estandarización de protocolos de seguridad, un aumento en la inversión en infraestructura digital y una reducción en la vulnerabilidad de sistemas críticos. Su naturaleza y difícil atribución han puesto en cuestión los límites entre lo que constituye un simple ataque informático y lo que podría considerarse un acto de guerra.
Asimismo, mecanimos como el Centro de Excelencia de Ciberdefensa Cooperativa de la OTAN (CCDCOE) y la Directiva NIS de la Unión Europea han facilitado el intercambio de información, la capacitación técnica y la creación de equipos de respuesta rápida, lo que ha mejorado significativamente la capacidad de detección temprana y mitigación de ataques en varios Estados miembros.Este debate cobra especial relevancia al debatir sobre cómo los ciberataques pueden tener consecuencias devastadoras sin verse como un acto de guerra física.

A pesar de estos avances, los resultados también evidencian limitaciones, ya que muchos ataques continúan ocurriendo, lo que demuestra, que, aunque las políticas existentes han fortalecido la resiliencia digital, aún no garantizan una protección total ni una disuasión completamente efectiva.

Terminos Clave

1. **OTAN** (Organización del Tratado del Atlántico Norte): Alianza política y militar de 32 países de Norteamérica y Europa establecida en 1949 para garantizar la seguridad y libertad de sus miembros a través de la defensa colectiva.
2. **Guerra Fría:** Enfrentamiento político, ideológico y económico entre dos bloques liderados por EE. UU. (capitalista) y la Unión Soviética (comunista). Duró desde el final de la Segunda Guerra Mundial (1945) hasta la disolución de la URSS (1991).
3. **Guerra Digital**: Uso de ataques digitales por parte de un país para dañar los sistemas informativos más esenciales de otro país.
4. **Ciberataques**: Cualquier esfuerzo internacional para robar, exponer, alterar, deshabilitar o destruir datos, aplicaciones u otros activos a través del acceso no autorizado a una red, sistema informático o dispositivo digital.
5. **Ciberseguridad**: Se refiere a todas las tecnologías, prácticas y políticas para prevenir los ciberataques o mitigar su impacto. La ciberseguridad tiene como objetivo proteger los sistemas informáticos, las aplicaciones, los dispositivos, los datos, los activos financieros y las personas contra el rango warm y otros malware, las estafas de phishing, el robo de datos y otras ciberamenazas.
6. **Ciberdefensa**: La respuesta por parte de los gobiernos para garantizar la seguridad dentro del ciberespacio. Se engloba dentro de la ciberseguridad, un concepto más amplio.
7. **Ciberespacio**: Se refiere al mundo real o artificial generado mediante la conexión a internet.
8. **Hacktivismo**: La práctica de usar el hacking para promover causas políticas o sociales.
9. **Atribución**: Proceso de identificar quién está detrás de un ciberataque, algo difícil por el anonimato en el ciberespacio
10. **Artículo 5 de la OTAN**: Principio de defensa colectiva: un ataque contra un miembro es considerado un ataque contra todos.
11. **Ciber soberanía**: Derecho de los Estados a controlar y proteger su infraestructura digital y la información dentro de sus fronteras.
12. **Inteligencia cibernética:** El proceso de recopilar y analizar datos sobre amenazas potenciales para evitar daños a las redes o los sistemas de una organización.

13. **Desinformación Digital:** La creación, difusión o promoción intencionada de información falsa, inexacta o engañosa con el objetivo de influir en la opinión pública, obtener beneficios políticos o económicos o desestabilizar a individuos, instituciones o sociedades enteras.
14. **Resiliencia digital:** La capacidad de anticipar, resistir, recuperarse y adaptarse a condiciones adversas, tensiones, ataques o compromisos que utilizan o son posibilitados por los recursos cibernéticos.
15. **Cooperación Internacional en ciberseguridad**: La cooperación internacional en ciberseguridad es la colaboración conjunta y coordinación entre países, organizaciones y otros actores para proteger los sistemas y datos digitales a nivel global de amenazas cibernéticas. Su objetivo es fortalecer la defensa colectiva contra ataques como el ransomware y el cibercrimen.
16. **Ciberterrorismo**: El uso de tecnologías de la información para intimidar, coaccionar o causar daños a gobiernos o poblaciones, con el fin de lograr objetivos políticos o sociales.
17. **Ransomware**: Un tipo de malware que retiene como rehenes los datos confidenciales del dispositivo o el dispositivo de una víctima, amenazando con mantenerlos bloqueados, o algo peor, a menos de que la víctima pague un rescate al atacante.

Historia del Comité

La Organización del Tratado del Atlántico Norte (OTAN) se fundó en 1949 como una alianza de defensa colectiva para garantizar la seguridad y la libertad de sus miembros en Norteamérica y Europa. Creada en la Guerra Fría (1945-1991) , su principal misión era la contención de la amenaza soviética a través de la persuasión política y militar. El principio fundamental en el que se sustenta es el Artículo 5, el principio de defensa colectiva, que establece que un ataque contra un miembro es considerado un ataque contra todos. Este principio actúa como una poderosa disuasión contra agresiones armadas tradicionales.

Tras la disolución de la URSS en 1991, la OTAN redefinió su propósito para abordar nuevos retos de seguridad y expandió sus horizontes geográficos y funcionales. Sin embargo, el panorama de seguridad se mantiene en constante cambio y desarrollo debido a la rápida interconexión global y la creciente dependencia del ciberespacio y herramientas digitales. Todo

esto abrió un nuevo escenario para el conflicto: la Guerra Digital, definida como el uso de ataques digitales por parte de un país para dañar los sistemas informáticos esenciales de otro.

- **2007 (Estonia)**: Los ataques cibernéticos masivos contra la infraestructura de Estonia demostraron el potencial desestabilizador de las ciberamenazas. Este evento impulsó a la alianza a establecer el Centro de Excelencia de Ciberdefensa Cooperativa (CCDCOE) en Tallinn.
- **2014 (Cumbre de Gales)**: La ciberdefensa fue elevada a la categoría de tarea esencial de la alianza.
- **2016 (Cumbre de Varsovia):** La OTAN declaró formalmente el ciberespacio como un dominio operacional, al mismo nivel que los dominios terrestre, aéreo y marítimo.

A pesar de que el ciberespacio fue declarado un dominio operacional en 2016, la realidad es que la OTAN ha evitado establecer una doctrina clara o una acción definitiva. A pesar de sus avances, la OTAN sigue enfrentando constantes desafíos como la coordinación multinacional, para lograr un consenso entre todos los miembros es necesaria la coordinación estrecha entre múltiples países y diversas organizaciones. Sin embargo, las diferencias políticas, los enfoques de seguridad, y las capacidades entre los miembros pueden obstaculizar una postura unificada. Por otro lado, también se enfrentan a amenazas en forma de desinformación y operaciones de influencia que buscan debilitar la unión social y la confianza pública (AICAD Business School, 2024). Es importante recalcar que la OTAN tiene como fin asegurar la protección del ciberespacio aliado, aumentar la capacidad de las redes y sistemas y garantizar que sus miembros coordinen mejor sus defensas contra actores maliciosos en el espacio digital (NATO ACT, s.f.).

Contexto Histórico

Desde finales del siglo XX, con la expansión del Internet y las tecnologías digitales, el ciberespacio se ha convertido en un nuevo dominio estratégico junto a la tierra, el mar, el aire y el espacio. La primera evidencia del uso militar del ciberespacio se remonta a la década de 1990, cuando Estados Unidos y otras potencias comenzaron a desarrollar más herramientas defensivas y ofensivas en el ámbito digital. Sin embargo, fue en 2007 cuando Estonia sufrió un masivo ciberataque que paralizó miles de instituciones bancarias, gubernamentales e incluso medios de comunicación, lo cual marcó uno de los primeros ejemplos de cómo un ataque a través del uso

digital amenaza directamente la estabilidad de un Estado. A partir de entonces, la frecuencia de estos ataques empezó a incrementarse a lo largo de los años. Además, las filtraciones de datos, ataques de software y la manipulación de información en redes sociales han demostrado que las guerras modernas pueden liberarse sin disparar un solo proyectil. De igual manera, el hecho de que estos ataques pueden venir de cualquier parte del mundo y de personas y grupos anónimos hace que sean extremadamente difíciles de rastrear. Ante este panorama, instituciones como la ONU y la OTAN han empezado a discutir cómo aplicar el derecho internacional en el ciberespacio y si un ciberataque debe considerarse un acto de guerra. Debido a esto la ONU fomento diálogos acerca la manera de implementar el derecho internacional en el ciberespacio, incluyendo discusiones en el Consejo de Seguridad sobre peligros cibernéticos que tienen la capacidad de comprometer "la paz y la seguridad internacionales" (Stimson Center, 2024). De la misma forma la ONU aprobó en diciembre de 2024 un acuerdo internacional para luchar contra los crímenes cibernéticos, llamado La Convención de las Naciones Unidas contra la Ciberdelincuencia. Su propósito es potenciar la colaboración entre países en el análisis y la investigación, así como también perseguir delitos como el tráfico de datos, ransomware o fraude y hacer más sencillo el intercambio y extradición de evidencias entre países. Sin embargo, todavía no hay un acuerdo claro ni reglas definidas, lo que crea un vacío que pone en riesgo la seguridad mundial.

Situación Actual

Actualmente, la OTAN está marcada por una constante creciente y sofisticada ofensiva digital que ha elevado la ciberseguridad a una prioridad estratégica absoluta, impulsando a todos los miembros a tomar acción definitiva y contundente. Un ámbito en el que el anonimato, la velocidad y la ausencia de fronteras físicas no están presentes ha transformado por completo la naturaleza de las amenazas globales. La alianza reconoce que los ciberataques se han convertido en una amenaza constante contra la seguridad nacional, capaces de afectar estructuras críticas, comprometer datos sensibles y desestabilizar sistemas estatales sin necesidad de un enfrentamiento militar tradicional.

En los últimos años la frecuencia, capacidad y complejidad de estos ataques han aumentado significativamente. La OTAN, consciente de esta realidad, ha elevado la problemática a una prioridad absoluta, obligando a todos los estados miembros a reforzar sus capacidades

internas y a trabajar bajo un enfoque de cooperación colectiva. Todo esto con el fin de responder a un entorno donde actores estatales, grupos criminales transnacionales y organizaciones hackactivistas utilizan herramientas digitales para infiltrar redes gubernamentales, manipular sistemas financieros, robar información clasificada y realizar campañas de desinformación con impacto directo a sociedades enteras.

La alianza ya ha reconocido la importancia de este nuevo campo. Desde 2016, el ciberespacio está considerado un dominio operacional equiparable a los ámbitos terrestre, aéreo y marítimo, lo que refleja la magnitud de amenaza que una Guerra Digital representa para una nación y para la seguridad colectiva de esta misma. Sin embargo, pese a este progreso institucional, la OTAN aún no ha logrado establecer un principio claro ni un consenso definitivo sobre cómo responder a ciberataques de gran escala y si el Artículo 5 de defensa colectiva debería de aplicarse en situaciones estrictamente físicas o se debería de extender también a digitales.

Casos de Estudio

Caso de Estudio 1: El Ciberataque a Estonia (2007)

En 2007, Estonia sufrió uno de los ciberataques más grandes de la historia, afectando bancos, instituciones gubernamentales, medios de comunicación y sistemas de servicios esenciales. El ataque, atribuido ampliamente a actores vinculados a Rusia, paralizó al país durante semanas y evidenció cómo un ciberataque puede causar daños equivalentes a los de un ataque físico. Además, el ataque generó pérdidas económicas significativas debido a la interrupción de servicios financieros y comerciales, así como una disminución temporal en la confianza de inversionistas y ciudadanos en los sistemas digitales del país.

Este evento llevó a la creación del Centro de Excelencia de Ciberdefensa Cooperativa de la OTAN en Tallinn. Desde el ámbito legal y político, el caso impulsó reformas en las leyes de ciberseguridad de Estonia y fortaleció su liderazgo dentro de la OTAN en temas digitales. El caso abrió el debate sobre si un ciberataque masivo debería activar el artículo 5 y si la OTAN debe considerar la infraestructura digital como parte de su defensa colectiva (BBC News, 2007).

Caso de Estudio 2: Inferencia Electoral y Desinformación en Estados Unidos y Europa.

Varios países miembros de la OTAN, incluidos Estados Unidos, Alemania, Francia y el Reino Unido, han denunciado campañas de ciberataques y desinformación ejecutadas por actores estatales extranjeros- principalmente Rusia- para influir en procesos democráticos. Estas campañas incluyen robo de correos electrónicos, hackeo de servidores de partidos políticos, manipulación de redes sociales y difusión masiva de noticias falsas. Estas acciones han generado costos económicos relacionados con la protección de sistemas electorales, investigaciones oficiales y el fortalecimiento de plataformas digitales contra la manipulación.

Esto plantea un desafío grande y crítico pero también abre el debate sobre los límites entre libertad de expresión, soberanía digital y seguridad nacional. En el ámbito político y legal, estos casos han provocado reformas en leyes electorales, mayor regulación de redes sociales y tensiones diplomáticas entre países involucrados, afectando la estabilidad institucional y la confianza ciudadana en los procesos democráticos (United States Senate Select Committee on Intelligence, n.d.).

Caso de Estudio 3: El ataque a Oleoductos y Energía Crítica (Colonial Pipeline, 2021)

En 2021, un grupo de hackers conocido como Dark Side lanzó un ransomware contra Colonial Pipeline, una infraestructura energética estratégica en Estados Unidos. El ataque obligó a cerrar el suministro de combustible a varios estados, provocando escasez, compras de pánico y pérdidas económicas millonarias. Aunque el ataque fue realizado por un grupo criminal no estatal, Estados Unidos denunció que operan desde territorio ruso, evidenciando el problema de la atribución en el ciberespacio.

<u>Temas para Discutir:</u>

1. **Atribución, responsabilidad estatal y actores no estatales**
    - Creación de estándares internacionales para determinar responsabilidad en ciberataques.
    - ¿Cómo manejar ataques de grupos hacktivistas o criminales no afiliados claramente a un Estado?

- Herramientas para asegurar transparencia en la atribución.
- ¿Qué responsabilidad tienen los Estados de origen sobre grupos criminales que actúan desde su territorio?

2. **Protección de infraestructura crítica**
    - ¿Qué sectores deben considerarse infraestructura crítica dentro de la OTAN? (energía, salud, bancos, defensa, etc.)
    - Coordinación entre países para proteger redes compartidas o interdependientes.
    - Regulaciones obligatorias de seguridad para infraestructura civil.
    - ¿Debe la OTAN considerar la desinformación digital y la manipulación de elecciones como una amenaza militarizada?
    - ¿Debería aplicarse la activación del Artículo 5 aun cuando el ataque no provenga oficialmente de un Estado? mmm
3. **Riesgos del desarrollo de ciberarmas ofensivas**
    - Riesgos del desarrollo de ciberarmas ofensivas.
    - ¿Debe la OTAN establecer límites o regulaciones internas sobre capacidades ofensivas?
    - Concepto de “ciber discusión ” y su efectividad.
4. **Desinformación y guerra psicológica digital**
    - Estrategias de la OTAN para combatir campañas de desinformación dirigidas a dividir sociedades.
    - Protección de procesos democráticos, elecciones y opinión pública.
    - Rol de empresas tecnológicas en la seguridad digital transnacional.

5. **Cooperación internacional en ciberseguridad**
    - Coordinación entre miembros en tiempo real: intercambio de inteligencia, respuesta rápida, entrenamiento.
    - Participación de países no miembros pero vulnerables (como Ucrania, Georgia o Finlandia antes de unirse).
    - Papel de organizaciones como la ONU, la UE y el CCDCOE.
6. **Derechos humanos y privacidad frente a la seguridad digital**

- ¿Hasta dónde pueden los gobiernos monitorear datos para asegurar la ciberdefensa?
- Protección de los ciudadanos ante vigilancia masiva o abuso gubernamental.
- Balance entre ciberseguridad estatal y libertades civiles.

Posiciones de Bloque:

Bloque Pro-Defensa Colectiva Digital

Países Líderes: Estados Unidos y Reino Unido

Este bloque considera que los ciberataques son un peligro para la seguridad de un país y para la estabilidad en el mundo. Los países que lo conforman creen que los ataques informáticos muy graves, especialmente los que afectan a cosas muy importantes como la infraestructura, el sistema financiero o los procesos democráticos, deben ser considerados tan graves como un ataque militar normal. Defienden que la OTAN debe contar con una postura firme, coordinada y disuasiva en el ciberespacio, incluyendo la posibilidad de aplicar el Artículo 5 en casos extremos. Para este bloque, la disuasión digital sólo es efectiva cuando existe una capacidad clara de respuesta colectiva. Asimismo, promueven el fortalecimiento del intercambio de inteligencia, la cooperación con el sector privado y el desarrollo de capacidades ofensivas y defensivas para proteger el orden democrático y la estabilidad euroatlántica (NATO,2024)

Bloque de Neutralidad estratégica y Soberanía Digital

Países Líderes: Francia y España

Este bloque comprende la severidad de los ataques cibernéticos y reconoce que son un problema grave para la seguridad de todos. Sin embargo, cree que actuar con demasiada prisa puede causar problemas a gran escala que no son necesarios, lo cual puede llevar a que la OTAN tenga menos autoridad a nivel internacional. Desde su punto de vista, sin pruebas claras y verificables, cualquier respuesta colectiva corre el riesgo de basarse plenamente en suposiciones o presiones políticas. Por ello, defienden que la activación del Artículo 5 debe ser una medida excepcional, aplicada sólo en circunstancias extremas y con consenso pleno.

Este bloque prioriza el fortalecimiento de las capacidades nacionales antes de delegar responsabilidades a nivel de alianza. Consideran que cada Estado debe tener sistemas sólidos de defensa que les permitan afrontar estos ataques cibernéticos junto con protocolos internos y personal capacitado, para no depender solo de mecanismos externos. Además, hacen énfasis en que la ciberseguridad debe tener en cuenta los principios del derecho internacional, la soberanía estatal , la privacidad y los derechos humanos. Tienen miedo de que si el poder colectivo crece a gran escala, se debilitará la supervisión democrática y los ciudadanos perderán la confianza (NATO, 2024)

Bloque de Innovación y Resiliencia Tecnológica

Países líderes: Finlandia y Canadá

Este bloque se centra principalmente en la prevención de problemas, la preparación y el desarrollo tecnológico como pilares fundamentales de la ciberseguridad. Creen fuertemente que la mejor defensa no es reaccionar esporádicamente después de un ataque, sino reducir al máximo las vulnerabilidades antes de que puedan ser usadas en su contra. Desde esta postura consideran que la inversión en investigación, inteligencia artificial, sistemas predictivos, simulaciones y ejercicios conjuntos, son esenciales para anticipar amenazas. Promueven el fortalecimiento del CCDCOE como centro de innovación, análisis y capacitación para todos los Estados miembros.

Ademas, apoyan la creación de estandares

Bloque de Defensa Multinivel

República Checa y Portugal

Este bloque presenta un sistema de respuesta organizado y por etapas. Esto ayuda a distinguir entre diferentes tipos de amenazas en el mundo digital. No todos los ataques tienen el mismo efecto o la misma intención. Por eso, no deberían recibir la misma respuesta. Defienden la creación de una escala de severidad digital que clasifique los ataques según su origen, impacto, duración y objetivos. A partir de esta clasificación, se determinará el tipo de respuesta más adecuada, que puede ir desde asistencia técnica hasta acciones diplomaticas o militares.

Este enfoque trata de evitar respuestas exageradas que puedan empeorar los problemas sin necesidad. Al mismo tiempo, permite tomar medidas firmes cuando los ataques son demasiado graves. Además, este bloque enfatiza la importancia de apoyar a los Estados con menos capacidad tecnológica. Consideran que una defensa colectiva sólo es efectiva si todos los miembros cuentan con herramientas mínimas de protección. Para este bloque es crucial encontrar un buen equilibrio entre trabajar juntos, tomar decisiones propias y asegurarse de que cada país contribuya de manera justa. Esto es fundamental para que la alianza sea capaz de funcionar de manera unida y efectiva.

Bloque Enfocado en Derechos Humanos y Privacidad

Países Líderes; Luxemburgo e Islândia

Este bloque prioriza la protección de las libertades fundamentales frente al crecimiento de medidas de vigilancia y control digital. Consideran que la seguridad es importante, pero creen que el uso excesivo de tecnologías de monitoreo puede debilitar la democracia y erosionar la confianza pública en las libertades fundamentales. Desde su perspectiva, muchas políticas de ciberseguridad actuales corren el riesgo de normalizar la vigilancia masiva, el almacenamiento indiscriminado de datos y el uso poco transparente de algoritmos.

Defienden la creación de organismos independientes que supervisen todo. Quieren auditorías periódicas para asegurarse de que todo se hace correctamente. También consideran que se necesitan marcos legales claros que digan cómo se pueden usar las tecnologías digitales. Apoyan leyes muy estrictas para proteger los datos de las personas y quieren mecanismos efectivos que hagan que las personas rindan cuentas de lo que hacen. Promueven la educación digital y el pensamiento crítico como herramientas clave para combatir la desinformación sin recurrir a la censura. Esto se debe a que consideran que una ciudadanía informada es una de las mejores defensas frente a la manipulación. La educación digital y el pensamiento crítico son fundamentales para que las personas puedan evaluar la información de manera efectiva y tomar decisiones informadas. Esto ayuda a prevenir la propagación de la desinformación y a fomentar una ciudadanía más consciente y crítica.

Posibles soluciones

1. Creación de un Protocolo de Respuesta Cibernética de la OTAN el cual consiste en establecer un documento oficial que defina niveles de ataque, procedimientos de evaluación, mecanismos de atribución y tipos de respuesta aplicables en cada caso. Esto permitiría actuar con rapidez y reducir improvisaciones.
2. Fortalecimiento del Centro de Excelencia en Ciberdefensa (CCDCOE) Ampliar sus funciones para incluir monitoreo permanente, simulacros obligatorios, análisis predictivo y capacitación continua para todos los estados miembros.
3. Sistema Unificado de intercambio de Inteligencia Digital. Crear una plataforma segura que permita compartir información sobre amenazas en tiempo real entre los miembros, reduciendo tiempos de respuesta y aumentando la coordinación.
4. Establecimiento de Estándares Mínimos de Seguridad. Implementar requisitos obligatorios para proteger infraestructura crítica, incluyendo auditorías periódicas, certificaciones técnicas y protocolos de emergencia.
5. Marco Legal para la Aplicación del Artículo 5 Digital, desarrollando criterios jurídicos claros que definan cuándo un ciberataque puede considerarse un acto de agresión colectiva, evitando interpretaciones subjetivas.
6. Fortalecer la cooperación con empresas tecnológicas, proveedores de servicios y expertos en ciberseguridad para prevenir ataques y mejorar sistemas defensivos.
7. Implementar campañas dirigidas a funcionarios, estudiantes y ciudadanía para reducir vulnerabilidades humanas como la desinformación.
8. Creación de Órganos de Supervisión Independientes: Establecer mecanismos de control que garanticen que las medidas de seguridad respeten los derechos humanos y eviten abusos de poder.

Referencias

About us. (s. f.).https://ccdcoe.org/about-us/

International Conference on Cyber Conflict – CyCon. (s. f.). https://ccdcoe.org/cycon/

Collective defence and Article 5. (s. f.). Site Name Seo. https://www.nato.int/en/what-we-do/introduction-to-nato/collective-defence-and-article-5

Cyber defence. (s. f.). Site Name Seo. https://www.nato.int/en/what-we-do/deterrence-and-defence/cyber-defence

Home page. (s/f). Cisa.gov.https://www.cisa.gov/?utm

Home | ENISA. (2025, 17 diciembre).https://www.enisa.europa.eu/?utm#contentList

Countering hybrid threats. (s. f.). Site Name Seo. https://www.nato.int/en/what-we-do/deterrence-and-defence/countering-hybrid-threats

(S/f). Canada.ca. https://www.canada.ca/en/department-national-defence/news/2025/11/cafcybercom-participates-in-natos-exercise-cyber-coalition-25.html

(S/f-b). Euronews.com. https://es.euronews.com/next/2025/10/21/ciberataques-rusos-paises-otan-aumentado-microsofthttps://www.pm.gc.ca/en/news/statements/2024/07/10/washington-summit-declaration

Newsroom Infobae. (2025, 18 julio). La OTAN condena una campaña de ciberataques rusos contra Ucrania y aliados para desestabilizar la alianza. *Infobae*. https://www.infobae.com/america/agencias/2025/07/18/la-otan-condena-una-campana-de-ciberataques-rusos-contra-ucrania-y-aliados-para-desestabilizar-la-alianza/

Reuters. (2024, 25 noviembre). Rusia no nos intimidará con ciberamenazas, dice ministro británico a la otan. *LA NACION*. https://www.lanacion.com.ar/agencias/rusia-no-nos-intimidara-con-ciberamenazas-dice-ministro-britanico-a-la-otan-nid25112024/

Statement by the North Atlantic Council concerning malicious cyber activities. (2020, 3 junio). Official Texts And Resources | NATO.

https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2020/06/03/statement-by-the-north-atlantic-council-concerning-malicious-cyber-activities

Aicad Business School. (2024, 22 julio). *Centro Integrado de Ciberdefensa: Estrategia de Ciberseguridad para la OTAN.* https://www.aicad.es/centro-integrado-de-ciberdefensa?utm

Cyber defence. (s. f.-b). Site Name Seo. https://www.nato.int/en/what-we-do/deterrence-and-defence/cyber-defence?utm

Home | ENISA. (2025b, diciembre 17).https://www.enisa.europa.eu/

Campaigns, S. (s/f). *Select committee on intelligence United States senate*. Senate.gov.https://www.intelligence.senate.gov/wp-content/uploads/2024/08/sites-default-files-documents-report-volume2.pdf

BBC NEWS | Europe | Estonia hit by «Moscow cyber war». (s. f.). http://news.bbc.co.uk/2/hi/europe/6665145.stm