



COMITÉ DE DESARME Y SEGURIDAD INTERNACIONAL

SIMUN XVII EDICIÓN

AUMENTO DE USO DE ARMAS CIBERNÉTICAS ENTRE NACIONES

GUÍA DE ESTUDIO



Estimados delegados,

Para el Comité Organizador, Equipo de Asesores y la Directiva de la institución, es un gran honor recibirlos en la decimoséptima edición de San Ignacio Model of United Nations. Nos llena de felicidad que puedan asistir a nuestro querido modelo, en el que buscamos transmitir nuestros valores: Empatía, Responsabilidad, Integridad y Constancia.

Este año, celebramos el vigésimo segundo aniversario de SIMUN. Durante esos años, la institución se ha caracterizado por marcar a jóvenes, los cuales han dejado un legado que sirve de inspiración para las nuevas generaciones. Nuestro objetivo es formar líderes que, en un mundo tan polarizado, disfruten de las diferencias en lugar de verlo como algo que nos separe. Por lo mismo, la situación general de esta edición del modelo será: “Rivalidades Históricas entre Regiones”.

Cada uno de los once comités en los que se estará debatiendo este año es prueba de la importancia de buscar la paz a nivel mundial en cada una de las oportunidades que se presenten. Desde las acciones y decisiones de nuestro día a día hasta en los proyectos globales, se puede generar un cambio con acciones que promuevan la tolerancia y la empatía. Estos son una necesidad crítica ante cómo las rivalidades llevan a conflictos cada vez más frecuentes.

Tomar la decisión de delegar en un modelo parece sencillo; sin embargo, requiere valor, asistir un fin de semana para debatir problemas que muchas veces son ignorados, con un proceso de investigación previo y discutiendo con personas que no conoces, pero estando abierto a tener un fin de semana diferente. Son cada uno de esos factores lo que le dan un valor especial a hacer MUN, haciendo que, para los que nos adentramos a este mundo, se marque un antes y un después que nos lleva a definir quienes somos y que es lo que nos apasiona.

El objetivo de esta edición de SIMUN es que puedan soñar con lo más grande; como dice la frase de la institución: “El Hombre es del Tamaño de sus Sueños”. La pieza clave de este modelo es que se reten a ustedes mismos a superarse, para poder cerrar el modelo sabiendo que aprendieron y mejoraron durante la competencia, no solo como delegados, sino como personas. Aprovechen los tres días de debate para disfrutar y crear recuerdos imborrables, que a la larga serán los momentos que se anhelan cuando, como es mi caso, se está acabando una hermosa etapa, la cual desde que entré en sexto grado me ha dado los mejores momentos de mi vida. ¡Nos vemos en SIMUN 2025!

Gabriel Gabizón Strumskis
Secretario General SIMUN 2025



Queridos delegados;

Primero que nada, quiero darles la bienvenida a la decimoséptima edición de nuestro Modelo de las Naciones Unidas. Estoy muy emocionada de tener la oportunidad de ser su presidenta durante estos tres días y no puedo esperar para conocerlos. Estoy segura de que no solo encontrarán una solución a este conflicto, sino que también vivirán una experiencia inolvidable.

Esta organización no solo se ocupa de regular las armas, sino que busca la paz que todos merecemos y la igualdad que tanto anhelamos. Ha defendido los derechos de los civiles y ha trabajado arduamente por una mayor seguridad en cada uno de sus países miembros. En este comité de DISEC, nos enfrentaremos a un desafío urgente: el creciente uso de armas cibernéticas. Este tema requiere una comprensión profunda de las complejidades geopolíticas, tecnológicas y éticas que lo rodean.

Como su mesa y junto con sus otros miembros, esperamos de ustedes un debate completo y constructivo, por eso los animo a presentarse como delegados completos que no solo han investigado a fondo sus posiciones, sino que también tienen la creatividad y originalidad para proponer soluciones innovadoras. Busco delegados que cuenten con una narrativa clara y convincente, capaces de expresar sus ideas de manera persuasiva.

Recuerden que DISEC tiene atribuciones específicas: abordar las amenazas a la seguridad internacional y promover el desarme. Sus soluciones deben ser realistas, viables y alineadas con las funciones de este comité. Sin embargo, tengan en cuenta que el tema que vamos a discutir en este comité está en desarrollo.

No se limiten a repetir las posturas típicas; desafíen el status quo, exploren nuevas perspectivas y trabajen juntos para construir ese futuro más seguro y pacífico; la información que tenemos es limitada, así que siéntanse libres de ser creativos, siempre dentro de un marco realista, pero con propuestas originales. Recuerden que deben conseguir un enfoque tanto social como político, económico y militar.

No duden en acercarse a nosotros con cualquier pregunta, inquietud o idea. Sabrina, Andrés, Juan y yo nos comprometemos a apoyarlos en el antes durante y después del modelo, juntos, podemos hacer de este comité una experiencia inolvidable.

Les deseo mucho éxito y espero con ansias conocerlos y escucharlos.

Con cariño,

Clementina Hernández
Presidenta de Mesa
clementina.hernandez.2026@colegiosi.org

Historia del Comité

El Comité de Desarme y Seguridad Internacional (DISEC) de las Naciones Unidas (ONU) fue creado como el primero de los Comités Principales de la Asamblea General cuando se firmó la Carta de las Naciones Unidas en 1945, fue creada como una comisión formada por todos los estados miembros con un compromiso de una reunión constante para la discusión de diversos temas, con base en el artículo 11 de la Carta de las Naciones Unidas. DISEC se formó para responder a la necesidad de un foro internacional para debatir cuestiones de paz y seguridad entre los miembros de la comunidad internacional.



La Asamblea General, por medio de su resolución 502 (VI) de enero de 1952, creó la Comisión de Desarme de las Naciones Unidas que quedó bajo la dirección del Consejo de Seguridad, con un mandato general sobre cuestiones relativas al desarme. Sin embargo, para 1959 la Comisión no tuvo un papel predominante, y para 1978, se estableció “una nueva Comisión de Desarme como órgano subsidiario de la Asamblea integrada por todos los Estados Miembros de las Naciones Unidas”.

Desde ese momento, se estableció la función de la Comisión como aquella de seguimiento y de elaboración de recomendaciones en materia de desarme y seguridad internacional.

Su propósito en la Asamblea General es establecer los principios generales de cooperación en el mantenimiento de la paz y la seguridad internacionales, incluidos los principios que rigen el desarme y la regulación de los armamentos, y también dar recomendaciones con respecto a dichos principios a los Miembros o al Consejo de Seguridad. Cabe recalcar que DISEC no puede asesorar directamente al Consejo de Seguridad en su proceso en la toma de decisiones, pero puede sugerir temas específicos para su consideración por el Consejo de Seguridad.

Además de su papel en la Asamblea General, DISEC también es una institución de la Oficina de las Naciones Unidas para Asuntos de Desarme (UNODA), nombrada formalmente en enero de 1998 después del segundo período extraordinario de sesiones del Secretario General sobre desarme en 1982. La UNODA se ocupa del desarme en todos los niveles (armas nucleares, armas de destrucción masiva y armas convencionales) y ayuda al DISEC a través de su trabajo realizado en la Asamblea General para brindar apoyo sustantivo en el establecimiento de normas para promover sus iniciativas de desarme. El Comité trabaja en estrecha cooperación con la Comisión de Desarme de las Naciones Unidas y la Conferencia de Desarme, con sede en Ginebra.

DISEC se ocupa del desarme, de los desafíos globales y de las amenazas a la paz, buscando soluciones a los desafíos del régimen de seguridad internacional. Se encarga de examinar todos los asuntos de desarme y seguridad internacional dentro de los ámbitos y funciones que posee, los principios generales de cooperación en el mantenimiento de la paz y la seguridad internacionales, así como los principios que rigen el desarme y la regulación de los armamentos; la promoción de acuerdos de cooperación y medidas encaminadas a fortalecer la estabilidad mediante niveles más bajos de armamentos.



Algunos de sus mayores logros, además de reunir a la comunidad internacional en pro del desarme en aras de la seguridad internacional, ha sido lograr el Tratado de No Proliferación Nuclear (TNP, el cual fue adoptado en 1970 y fue ratificado por más de 190 Estados (IAEA, 2020). Además, también ha realizado el Tratado sobre el Comercio de Armas (TCA), el cual entró en vigor el 24 de diciembre de 2014 y ya ha sido ratificado por más de 83 Estados. DISEC ha sido una Comisión que se ha encargado de coordinar y regular el uso de armas con el fin de evitar la repetición de los desastres y atrocidades como los

que dejó la Segunda Guerra Mundial para países y poblaciones enteras.

Esta comisión ha buscado, a través de los años, concentrarse en temáticas de vital relevancia para la comunidad internacional, enfocándose en regular exhaustivamente las diversas amenazas que surgen para los individuos con el desarrollo de la tecnología armamentística. Entre los problemas que DISEC ha buscado soluciones se encuentra en primer lugar, y estrechamente relacionado con el contexto histórico y político en el que se crearon las Naciones Unidas, están las armas nucleares. A pesar de que llegar a una desnuclearización total es prácticamente imposible, se ha logrado un progreso considerable. Sobresale, por ejemplo, el establecimiento de una ZLAN (Zona Libre de Armas Nucleares) en América Latina, consolidada en el Tratado de Tlatelolco. Por otro lado, está el Tratado de Prohibición Completa de los Ensayos Nucleares, que como indica su nombre, busca detener las pruebas de armamento nuclear. El comité también ha buscado erradicar el uso de armas de destrucción masiva, entre las que se encuentra el armamento químico y biológico. Por otro lado, las armas convencionales han sido reguladas de forma exhaustiva.

DISEC y sus miembros han buscado combatir problemas contemporáneos, tales como el tráfico ilícito de armas ligeras y el comercio de armas en general. El tratado que abarca estos problemas de forma más eficiente es el ATT (Arms Trade Treaty), expedido en el 2012. Con el paso del tiempo, esta

comisión ha debido adaptarse a las nuevas tecnologías, razón por la cual ha desviado su atención hacia temas más recientes, como, por ejemplo, la seguridad en el espacio exterior. Así, se han discutido temas como la prevención de una carrera armamentística en el espacio. Igualmente se han aprobado resoluciones, tales como la 69/32, que buscan evitar la instalación de armas en el espacio exterior.



Por último, DISEC también ha centrado su atención en múltiples temáticas tales como el rol de la tecnología en la seguridad. Asimismo, ha buscado medidas para que los países sean más transparentes con sus gastos militares. Además, ha llevado a cabo acciones en aras de fomentar la creación de centros para la paz y el desarme en diversas regiones.

En síntesis, la Organización de las Naciones Unidas ha regulado, con el paso del tiempo, los temas más relevantes en materia de desarme y seguridad, siempre teniendo en cuenta valores fundamentales como la cooperación internacional, la transparencia y la paz.

Antecedentes

La ciberseguridad no nació hasta que se comenzaron a conectar los equipos y a desarrollarse redes de

computadoras, lo cual ocurrió en 1950, cuando se crearon las primeras redes informáticas y módems. Fue en 1960 cuando la ciberseguridad comenzó a tomar la forma que conocemos en la actualidad. Con este contexto podemos separar la primera parte de la historia de esta disciplina en dos partes: antes y después de la invención del Internet. Antes del Internet, la única forma de dañar un dispositivo era acceder físicamente a él, por lo tanto, el delito era considerado como “allanamiento de morada” y no ciberataque. Después de la invención del Internet a finales de los 60 fue cuando nace el ciberespacio, lo que significó un nuevo entorno y una nueva posibilidad para los ciberdelincuentes.

A medida que las empresas empezaron a utilizar la web, controlar el acceso a los datos en los sistemas se convirtió en un punto importante de preocupación a mediados o finales de la década de 1960, dando el inicio a la implementación de la seguridad informática. Entre las primeras medidas para proteger la información se incluye el procesamiento de periodos, donde se separaban las actividades por partes y los usuarios podían manipular la información en un tiempo determinado, establecido por los expertos de ciberseguridad.



Según Prieto (2025), en 1970 “el investigador Bob Thomas desarrolló un programa informático llamado Creeper, que podía moverse a través de la red de ARPANET (la primera red de computadoras) y para evitar esto, Ray Tomlinson, el creador del correo electrónico, desarrolló el programa Reaper, que se encargaba de perseguir y eliminar a los Creepers. Reaper fue el primer sistema antivirus de malware y el primer programa con la capacidad de autorreplicarse, es decir, fue el primer virus y a partir de esto se crearon los primeros gusanos y troyanos informáticos. Sin embargo, fue en 1978 que nacieron los primeros programas maliciosos comerciales que examinaran los virus para posteriormente con el avance tecnológico proteger los sistemas de posibles daños.”

A principios de la década de 2000, las organizaciones criminales comenzaron a financiar en gran medida los ataques cibernéticos profesionales y los gobiernos comenzaron a tomar medidas drásticas contra la ciberdelincuencia. En estos años la Seguridad Informática comenzó a avanzar, pero lamentablemente también los virus y los programas maliciosos también fueron sofisticándose.

En abril de 2007, Estonia sufrió un ataque DDoS masivo que paralizó servicios bancarios, medios y gubernamentales durante días. Atribuido a grupos pro-rusos, este incidente demostró cómo actores estatales podían emplear tácticas cibernéticas para desestabilizar un país sin intervención militar directa. El evento se convirtió en

un caso de estudio para la OTAN, impulsando debates sobre la necesidad de protocolos de defensa colectiva.



En ese mismo año, el *Aurora Generator Test*, en el Laboratorio Nacional de Idaho, mostró que un ciberataque podría destruir infraestructura física, dañando un generador diésel mediante la manipulación de su sistema de control. Según Bloxberg (2024) “Este experimento evidenció el potencial destructivo de las armas cibernéticas más allá del ámbito digital. En 2010, el descubrimiento de Stuxnet, un malware diseñado para sabotear centrifugadoras nucleares iraníes, marcó un punto de inflexión.” Desarrollado presuntamente por EE.UU. e Israel, Stuxnet validó las ciberarmas como herramientas no letales pero estratégicas, capaces de impactar programas militares sin violar abiertamente acuerdos internacionales. Las filtraciones de Edward Snowden en 2013 expusieron programas de vigilancia masiva como PRISM, generando debates sobre el equilibrio entre seguridad nacional y privacidad. Esto inspiró a otros estados a intensificar sus capacidades de ciber espionaje.

Entre 2014 y 2016, ciberataques vinculados a Rusia afectaron procesos electorales en EE.UU., Francia y Alemania, buscando influir en resultados y erosionar la confianza en instituciones democráticas.

En 2017, los ataques NotPetya y WannaCry ilustraron cómo las ciberarmas podían causar daños colaterales masivos. NotPetya afectó empresas globales como Maersk y Merck, con pérdidas superiores a \$10 mil millones, mientras que WannaCry paralizó sistemas de salud en el Reino Unido y otros países.

En 2022, la guerra entre Rusia y Ucrania convirtió a Ucrania en un campo de pruebas para tácticas cibernéticas integradas con operaciones militares. Ataques a redes eléctricas y sistemas bancarios buscaban debilitar la resistencia civil y militar. Rusia empleó *bots* y *deepfakes* para difundir propaganda, mientras Ucrania contraatacó con apoyo de hacktivistas internacionales. Durante el invierno ucraniano de 2023, ataques a sistemas de calefacción y energía dejaron a poblaciones sin servicios básicos, violando principios del derecho humanitario internacional.



Según ManageEngine (2025), “Estos eventos reforzaron la necesidad de regulaciones globales, ya que el 80% de los miembros de la OTAN identificaron las ciberarmas como amenazas prioritarias para la seguridad

nacional. En 2024, la integración de inteligencia artificial en sistemas de defensa permitió detectar y neutralizar amenazas en tiempo real, pero también facilitó la creación de malware adaptativo, aumentando la complejidad de los ataques. Todos estos ataques vienen dados por causas políticas, en los que se interfieren en procesos electorales, reduciendo de esta forma la confianza institucional”.

Según la Cybersecurity & Infrastructure Security Agency, aproximadamente el 70% de los ataques cibernéticos están dirigidos a sistemas electorales, buscando manipular procesos políticos y desestabilizar gobiernos. Estos ataques pueden incluir hackeos a partidos políticos y campañas de desinformación en redes sociales, como se vio en elecciones en EE.UU., Francia y Alemania entre 2014 y 2016. Además, el phishing y la ingeniería social son métodos comunes para acceder ilegalmente a redes, con más de 12 millones de correos electrónicos de phishing llegando a organizaciones estadounidenses en 2021.

Los ciberataques también se emplean como herramientas estratégicas para desestabilizar a naciones rivales sin recurrir a conflictos armados directos. Según Barracuda Networks (2023), “los datos de ciberseguridad y los procesos operativos son los más vulnerables a los ataques estatales, con un 42% y 41% de los ataques dirigidos a estos sectores, respectivamente. Además, países como Rusia, China y Corea del Norte son frecuentemente identificados como responsables de estos ataques, con un

39%, 35% y 28% de las organizaciones creyendo que estos países están detrás de los ataques.”

Planteamiento del Problema

La evolución de la tecnología ha avanzado lo suficientemente rápido para transformar la naturaleza de los conflictos que afectan a la comunidad internacional, uno de los más resaltantes es el del aumento masivo de armas cibernéticas las cuales se han convertido en herramientas clave presentes en la estrategia diaria de cada nación. Las mismas se han vuelto indispensables para la estrategia militar y de defensa nacional, sin embargo, las vastas posibilidades de uso de armas cibernéticas ya sea para la defensa o ataque, internacional o incluso nacional, llama la atención de quienes entienden el riesgo a la violación de derechos humanos que estas armas proponen.



Según un informe de la OTAN, el 80% de sus miembros considera las armas cibernéticas como una de las mayores amenazas para su seguridad nacional, resaltando un dilema moral sobre su uso en conflictos (OTAN, 2020). De esta manera el aumento del uso de armas cibernéticas entre naciones ha desatado una serie de preocupaciones que afectan no solo la seguridad

internacional, sino también la estructura política, militar y social de los estados.

El uso de armas cibernéticas está íntimamente relacionado con la inestabilidad política interna de las naciones. La capacidad de llevar a cabo ciberataques ha permitido a los actores estatales y no estatales influir en los procesos democráticos y desvirtuar la confianza pública en las instituciones. Un claro ejemplo de esto es el uso de ciberataques para interferir en elecciones, donde los datos muestran que más de la mitad de los ataques cibernéticos están dirigidos a sistemas electorales. Este tipo de interferencia no solo afecta el resultado de las elecciones, sino que también mina la legitimidad de los gobiernos electos, creando un ambiente de desconfianza y división dentro de la sociedad que da paso a la corrupción.

Además, los ciberataques pueden llevar al incumplimiento de acuerdos internacionales. Los estados pueden utilizar estas armas para desestabilizar a sus rivales sin necesidad de un conflicto armado directo. Este tipo de guerra no violenta no solo afecta a los gobiernos, sino que también tiene un impacto significativo en los civiles, creando un ambiente de desconfianza y sensación de inseguridad social que puede causar conflictos más amplios entre las naciones, llevando al desbalance en la aplicación de sanciones directas como consecuencia del desacuerdo entre ambas.

La manipulación de la opinión pública a través de ciberataques también

ha aumentado. Los estados pueden utilizar ciber espionaje para obtener información sobre oponentes políticos y luego desviar la atención hacia ataques que comprometen su imagen pública. Además, se ha documentado que la desinformación y la propaganda han sido utilizadas para influir en la percepción pública, afectando la estabilidad política y fomentando un clima de agitación social.

Esta problemática también afecta directamente al ámbito militar, las armas cibernéticas presentan un nuevo panorama de interferencia militar que amenaza directamente. Los estados pueden llevar a cabo sabotajes directos a la infraestructura militar de sus oponentes, comprometiendo sistemas de comunicación y operaciones estratégicas. Este tipo de sabotaje permite a los atacantes evitar confrontaciones físicas directas, mientras que las consecuencias de sus acciones pueden ser devastadoras para los atacados. Por ejemplo, los ataques cibernéticos a sistemas de defensa aérea han demostrado cómo un estado puede neutralizar la capacidad militar de otro sin disparar una sola bala.

Por otro lado, el uso de armas



cibernéticas también permite el sabotaje

de ataques y contraataques por parte del bando contrario. Esto crea una dinámica en la que los estados pueden frustrar los esfuerzos militares de sus adversarios sin necesidad de una confrontación abierta. Además, el papel de terceros en este contexto es crucial, ya que pueden intervenir en conflictos a través de ciberataques, ampliando así el espectro de la guerra moderna. La intervención externa en guerras civiles se ha facilitado por estas nuevas tecnologías, donde actores externos pueden influir en el conflicto sin estar físicamente presentes.

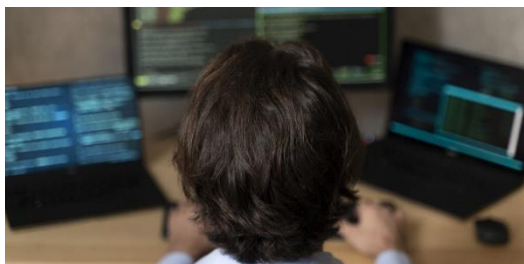
Los conflictos recientes, como el de Rusia y Ucrania, han ejemplificado cómo las armas cibernéticas pueden ser utilizadas para manipular la percepción pública y desestabilizar a un adversario. Los ataques a infraestructuras críticas, como las redes eléctricas y los sistemas de comunicación, han demostrado que la guerra cibernética puede tener efectos devastadores en la capacidad de un estado para defenderse.

Asimismo, llama la atención de la comunidad internacional la creciente afectación social que surge del uso abusivo de las armas cibernética, las cuales pueden ser vistas desde un punto más abstracto donde la amenaza se encuentra directamente en la integridad de las personas no realmente involucradas en el mundo político-militar actual. Los ciberataques pueden llevar al sabotaje de dinámicas socio-políticas internas, afectando la cohesión social y fomentando divisiones entre diferentes grupos. La manipulación de la opinión pública a través de redes sociales y otras plataformas digitales permite a

los estados o actores no estatales incitar al odio y promover agendas ideológicas, lo que a su vez puede resultar en violencia y conflictos internos.

El uso de plataformas tecnológicas civiles para manipular la educación y promover doctrinas ideológicas ha aumentado. La capacidad de difundir propaganda subliminal y desinformación se ha convertido en una herramienta poderosa para aquellos que buscan influir en la percepción pública y desestabilizar a los gobiernos. Este tipo de intervención no solo afecta la estabilidad política, sino que también plantea serias cuestiones sobre la ética y el respeto a los derechos humanos. La manipulación de ideales e incitación al odio a través de plataformas digitales ha mostrado cómo las armas cibernéticas pueden tener un impacto profundo en la cohesión social, llevando a la polarización y al extremismo.

Los efectos de estos ciberataques



no se limitan a la esfera política y militar; su impacto se extiende a la infraestructura social y los servicios críticos. Por ejemplo, los ataques a sistemas de salud y educación pueden tener repercusiones devastadoras en la vida cotidiana de los ciudadanos, creando un ambiente de miedo y desconfianza que puede socavar la estabilidad a largo plazo. La capacidad

de un estado para funcionar de manera efectiva se ve comprometida cuando sus servicios esenciales son blanco de ataques.

El uso creciente de armas cibernéticas plantea un desafío multifacético para la comunidad internacional. Los efectos de estos ataques no son solo estratégicos, sino que tienen implicaciones profundas en la política, la estructura militar y la cohesión social. A medida que los estados continúan desarrollando y utilizando estas herramientas, es imperativo que se establezcan mecanismos internacionales que regulen su uso y promuevan un entorno más seguro y estable. La cooperación global y el diálogo se convierten en elementos esenciales para abordar este fenómeno, creando un marco ético y legal que garantice que las armas cibernéticas no se utilicen para desestabilizar y socavar los principios fundamentales de la convivencia pacífica.

Acciones Pasadas

A lo largo de los siglos se han podido apreciar distintos tipos de ataques y de estrategias militares en contra de otro grupo armado, mientras que al principio se usaban técnicas más coloquiales como espadas y lanzas, el método evolucionó a las armas de fuego, y con el gran aumento de las tecnologías también se han desarrollado las armas cibernéticas también conocidas como ciberarmas.

Para desarrollar esta idea primero se tiene que conocer el significado de

que es una ciberarma para entender cómo funciona. Un arma cibernética es un malware desarrollado para objetivos militares, paramilitares o de inteligencia.

Un malware es un programa o software diseñado con fines maliciosos. Entre estos fines maliciosos podemos encontrar lo que es robar tus datos personales o privados e incluso formatear tu dispositivo electrónico, lo que al sucederle a un particular puede ser visto como un problema de precaución personal, pero el problema cambia cuando afecta a los sistemas de seguridad de una nación, haciendo posible el robo de la tecnología política y convirtiéndose en una amenaza mayor. Si ese malware no es correctamente aislado, en la seguridad online y la seguridad física, dos mundos completamente separados convergen y es en ese preciso momento donde se puede iniciar un proceso bélico mayor.

El primer malware desarrollado fue a lo largo de los años 80 cuando un grupo de jóvenes desarrolló el primer virus, el cual tenía como objetivo principal el divertirse, estos primeros virus se desarrollaron de manera inofensiva los cuales se podían arreglar reiniciando el dispositivo. Este juego empezado por un selecto grupo de jóvenes se fue transformando en un negocio. Donde al comienzo del siglo XXI, el dinero fue tomando posición en la actividad de hackeo, en donde aquel que era aficionado y le gustaba desarrollar softwares se convierte en profesional, donde este individuo podía trabajar por su cuenta, o al servicio dentro de una banda, o para algún

gobierno. Dependiendo del objetivo del individuo este se puede considerar con un ciber terrorista, como un hacktivista o como un hacker de sombrero blanco o de sombrero negro según sus intenciones.



Continuando con la idea, se ha desarrollado, hace unos cuantos años, la primera arma cibernética que se ha conocido en el planeta, Stuxnet, el cual supera cada uno de los malwares desarrollados hasta el momento. Este es considerado la primera ciberarma debido a que los malwares desarrollados previamente no se habían utilizado completamente para fines militares. Stuxnet es la primera arma de código el cual, al momento de ser descubierto, estaba repartido por todo el mundo, afectando así a todo tipo de infraestructuras, esto incluyendo a fábricas, controles de tránsito, a oleoductos y más importante para los países, sus centrales nucleares.

Este virus no solo era más complejo que cualquier virus anteriormente desarrollado, sino que este operaba, sin que nadie lo detectase, esto debido a que hacía creer a los dispositivos afectados que todo estaba en orden dentro del dispositivo.

Hoy en día Stuxnet es el responsable de que cada uno de los gobiernos en el mundo incluyan en sus sistemas la ciberdefensa como uno de los pilares fundamentales de la seguridad de las naciones

Este virus fue detectado en territorio bielorruso durante el transcurso del mes de junio en el año 2010 por un experto en software antivirus llamado Sergey Ulasen, cuando fue consultado por varios de sus clientes del territorio iraní, que había entrado en estado de pánico, debido a una cantidad de apagones inexplicables de los equipos de una de las centrales nucleares del territorio. Este código fue compartido con todas las empresas de desarrollo de antivirus, y el análisis preliminar realizado por un grupo de ingenieros de la empresa de desarrollo de antivirus, Symantec, mostró una cantidad y precisión de detalles nunca vistos hasta el momento.

Stuxnet poseía cuatro vulnerabilidades zero-day las cuales son las partes de código más cotizadas. Estas vulnerabilidades hacen posible que el dispositivo no tenga que realizar ninguna acción, ni clickear ni descargar. Estas piezas son las hacen que puedas acceder al sistema operativo. El precio que el paquete de vulnerabilidades zero-days poseía, el cual era cercano al medio millón de dólares, que pudo haber alcanzado en el mercado negro, hace que se reduzca la lista de posibles creadores del malware a solo tres:

- Cibercriminales tradicionales en busca de algún beneficio.

- Hacktivistas interesados en la diversión, el reto o el mensaje político.
- Naciones estados en busca de inteligencia de alto nivel o sabotaje.

A pesar del número de opciones, el nivel de sofisticación que poseía el virus, tomaba la sugerencia de que haya sido una nación, pero a pesar de eso los analistas de código no podían saber nada más.

A medida que pasaba el tiempo se podía observar el objetivo con el que los creadores habían desarrollado stuxnet. Este era un tipo de Hardware muy específico al cual se accedía mediante el software de control, supervisión y adquisición de datos de los PLC de la marca Siemens. Los PLC son los controladores lógicos programables, es decir, los equipos que se utilizan para el control de sistemas automatizados sin razón aparente.



Comenzaban a salir ciertas teorías de quienes, y como se había desarrollado Stuxnet, y por alguna razón siempre se encontraban los mismos involucrados. Una de las teorías apunta a la posible colaboración entre estados unidos e Israel, se dice que la participación de la Mossad (una de las agencias de

inteligencia israelíes) fue vital para colocar el virus en Natanz (20% de sus centrifugadoras quedó fuera de servicio). Existe otra teoría que va más lejos, que dice que la versión agresiva del malware fue una alteración unilateral de Israel, sin consulta ni aprobación de los Estados Unidos. Sea cual sea la teoría correcta, Stuxnet era un ataque en tiempos de paz, es decir una declaración de guerra, utilizando un armamento nunca antes visto. También hay que tener en cuenta que Stuxnet no es solo un malware que sabotea, sino que es capaz de causar explosiones que pudieran acabar con vidas humanas.

Stuxnet generó varias consecuencias, y una de ellas fue que Irán hoy en día posea uno de los mayores ciber ejércitos del mundo. La reacción a los incidentes causado en la central nuclear de Natanz, desencadenó un movimiento patriótico en el que miles de jóvenes iraníes se dedicaran a formarse y convertirse en ingenieros informáticos, y que ahora han puesto sus conocimientos al servicio del estado iraní. Al igual que todavía no se conoce la autoría del ataque de Stuxnet, tampoco se sabe la autoría de los más recientes a Saudí Aramco, la compañía petrolífera más grande del mundo, la cual sufrió un ataque que borró el código de 30.000 equipos y a los bancos como Bank of América, West Fargo, entre muchos otros, que sufrirían también un ataque de denegación de servicio y de filtración de datos privados, se sospecha que Irán pudo haber estado detrás de estos ataques.

Situación Actual

La seguridad internacional se encuentra en un punto crítico, marcado por un preocupante aumento en el desarrollo y uso de armas cibernéticas. A diferencia de las armas tradicionales, las cibernéticas operan en el ámbito digital, un espacio sin fronteras claramente definidas, lo que complica la tarea de atribuir ataques y aplicar las leyes internacionales que ya existen.

Como fue mencionado anteriormente, las armas cibernéticas abarcan una amplia gama de capacidades, desde el sabotaje de infraestructuras críticas (como redes eléctricas, sistemas de salud e instituciones financieras) hasta la manipulación de información y la interferencia en procesos democráticos. Esta versatilidad las convierte en herramientas muy atractivas para estados y actores no estatales que buscan ejercer poder o desestabilizar a sus enemigos sin los costos y la visibilidad de un conflicto armado.

Aunque la relación estado-nación sigue siendo el principal desarrollador y usuario de armas cibernéticas, la proliferación de actores no estatales, como grupos terroristas y organizaciones criminales, presenta desafíos adicionales. Estos grupos pueden adquirir o desarrollar capacidades cibernéticas bastante avanzadas, lo que les permite llevar a cabo ataques con un impacto considerable.

Uno de los mayores obstáculos para enfrentar la amenaza de las armas

cibernéticas es la dificultad de atribuir ataques con certeza. La naturaleza anónima de estos ataques permite a los perpetradores ocultar su identidad y su origen, lo que complica la implementación de medidas de respuesta y disuasión.

Además, la falta de un marco legal internacional claro y vinculante para regular el uso de armas cibernéticas crea un vacío legal que los estados y otros actores pueden aprovechar. Aunque existen algunos acuerdos y normas no vinculantes, como el Manual de Tallin sobre el Derecho Internacional Aplicable a la Guerra Cibernética, su aplicación y efectividad son limitadas.

El aumento en el uso de armas cibernéticas genera serias preocupaciones sobre la estabilidad internacional y los derechos humanos. Los ataques cibernéticos tienen el potencial de desestabilizar regiones enteras, interrumpir servicios esenciales y socavar la confianza en nuestras instituciones democráticas. Además, el uso de estas armas para la vigilancia masiva y la censura puede violar derechos fundamentales como la privacidad y la libertad de expresión.



Frente a esta creciente amenaza, es crucial que la comunidad

internacional tome medidas urgentes y coordinadas.

Esto implica:

Fortalecer la cooperación internacional: Los países deben trabajar juntos para compartir información, desarrollar capacidades de defensa cibernética y establecer normas y principios comunes que guíen un comportamiento responsable en el ciberespacio.

Promover la transparencia y la rendición de cuentas: Es esencial que los estados se comprometan a revelar sus capacidades cibernéticas y a ser responsables por sus acciones en el ciberespacio.

Desarrollar un marco legal internacional vinculante: La comunidad global debe esforzarse por crear un marco legal claro y obligatorio que regule el uso de armas cibernéticas y establezca normas para la atribución de ataques.

Proteger la infraestructura crítica: Los países deben invertir en la protección de su infraestructura vital contra ataques cibernéticos y colaborar con el sector privado para mejorar la ciberseguridad.

Fomentar la educación y la concienciación: Es fundamental educar a los ciudadanos sobre los riesgos asociados con las armas cibernéticas y promover una cultura de ciberseguridad responsable.

La amenaza de las armas cibernéticas es un desafío complejo y multifacético que exige una respuesta global integral, y como organización, solo a través de la cooperación y el compromiso colectivo se puede asegurar un ciberespacio seguro y estable para todos.

Casos de Estudio

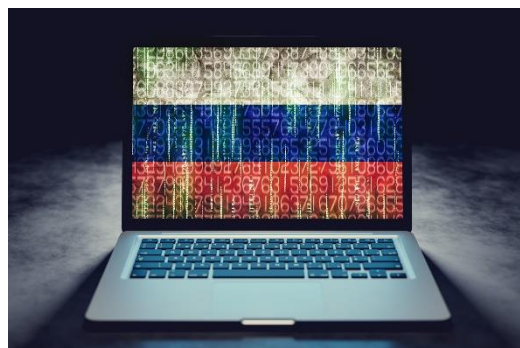
Guerra Ruso-ucraniana:

La guerra entre Ucrania y Rusia, que comenzó en 2014 con la anexión de Crimea, ha evolucionado hacia un conflicto prolongado caracterizado por la complejidad de las relaciones internacionales, la intervención militar y el uso de armas cibernéticas. Desde el inicio de las hostilidades, las tácticas cibernéticas han sido fundamentales para ambos lados, con Rusia utilizando ataques cibernéticos para desestabilizar al gobierno ucraniano y Ucrania respondiendo con sus propias capacidades defensivas. Este conflicto ha puesto en relieve cómo la guerra cibernética puede alterar las dinámicas de poder en un conflicto militar, creando un nuevo campo de batalla que trasciende lo físico.

Uno de los incidentes más notorios en este contexto fue el ciberataque conocido como Not Petya, que tuvo lugar en junio de 2017. Este ataque fue diseñado principalmente para afectar a Ucrania, comprometiendo sistemas de transporte, energía y finanzas. Se estima que No Petya costó a las empresas afectadas más de \$10 mil millones a nivel global (Symantec, 2018). La naturaleza del ataque, que se extendió rápidamente a otras naciones,

subraya cómo las armas cibernéticas pueden ser utilizadas no solo para fines militares, sino también como herramientas de desestabilización económica.

El ataque de Not Petya es emblemático de la estrategia rusa, que combina la guerra convencional con ataques cibernéticos. Según un informe del Centro de Análisis de Políticas Europeas (CEPA), “Rusia ha utilizado ciberataques como una extensión de su política militar, buscando desestabilizar a Ucrania desde dentro” (CEPA, 2020). Este tipo de guerra híbrida se caracteriza por la combinación de acciones militares tradicionales y operaciones cibernéticas, permitiendo a Rusia evitar confrontaciones directas mientras causa estragos en la infraestructura crítica de Ucrania.



El uso de armas cibernéticas por parte de Rusia no se ha limitado a ataques directos a la infraestructura. También incluye campañas de desinformación a través de redes sociales, diseñadas para influir en la opinión pública tanto en Ucrania como en Occidente. Un informe de la OTAN señala que “las operaciones de influencia rusa han sido diseñadas para socavar la confianza del público en el gobierno ucraniano y promover divisiones dentro

de la sociedad” (OTAN, 2021). Este enfoque multidimensional muestra cómo las tácticas cibernéticas pueden ser utilizadas para lograr objetivos políticos más amplios, socavando la legitimidad de un gobierno sin necesidad de un enfrentamiento militar directo.

La guerra en Ucrania ha resaltado la necesidad urgente de establecer un marco internacional que regule el uso de armas cibernéticas. La falta de normas claras permite que los estados actúen según sea conveniente para ellos mismos, utilizando estas armas para irrumpir en la soberanía de otros países.

La OTAN enfatiza que “las armas cibernéticas representan un desafío constante para la seguridad colectiva, y su uso en conflictos como el de Ucrania subraya la necesidad de cooperación internacional” (OTAN, 2021). Así a medida que el conflicto continúe, el uso de armas cibernéticas seguirá siendo un factor clave, y Ucrania deberá buscar la manera de adaptarse a este nuevo campo de batalla. Esto es un claro recordatorio para la comunidad internacional de que las armas cibernéticas pueden tener efectos devastadores en la estructura política, militar y social de un estado. Se debe abordar este problema mediante el establecimiento de normas y acuerdos que regulen el uso de armas cibernéticas, garantizando que se utilicen de manera que no eviten la paz y la estabilidad.

Golpe Militar de Myanmar (2021):

El golpe militar en Myanmar en febrero de 2021 marcó un punto de inflexión en la política del país, donde el ejército tomó el poder alegando fraude

electoral en las elecciones de noviembre de 2020. Este evento generó una respuesta masiva de protesta por parte de la población, que abogó por la restauración de la democracia. Sin embargo, el ejército birmano utilizó tácticas de represión y control cibernético para sofocar el disenso, destacando el uso de armas cibernéticas en un contexto de conflicto interno.



Desde el golpe, el ejército de Myanmar ha implementado un régimen de censura que incluye el bloqueo de plataformas de redes sociales y el monitoreo de la actividad en línea. Human Rights Watch indica que “las autoridades han utilizado la tecnología para suprimir la libertad de expresión, cerrando el acceso a las plataformas digitales y arrestando a activistas y periodistas” (Human Rights Watch, 2021). Este uso de ciber control permite al régimen militar mantener el control sobre la narrativa pública y limitar la capacidad de organización de los opositores.

El ejército ha empleado tecnología de vigilancia para rastrear a los activistas y disidentes. La organización Access Now ha documentado casos en los que las fuerzas de seguridad han utilizado datos recopilados de plataformas cibernéticas para identificar y arrestar a manifestantes

pacíficos (Access Now, 2021). Este tipo de intervención cibernética no solo infringe los derechos humanos, sino que también muestra cómo la guerra cibernética puede ser utilizada para mantener el control autoritario.

Por otro lado, los grupos de resistencia han empleado técnicas de ciberactivismo para contrarrestar la represión. Han utilizado redes sociales para organizar protestas y difundir información sobre las violaciones de derechos humanos cometidas por el ejército. Sin embargo, estas acciones también los han expuesto a represalias y ataques cibernéticos por parte del régimen, que busca dismantelar cualquier forma de resistencia.

El golpe militar de Myanmar ha revelado cómo las armas cibernéticas pueden ser utilizadas para sabotear dinámicas socio-políticas internas y para dismantelar movimientos de protesta. La falta de acceso a información imparcial y el control de la narrativa han permitido que el régimen militar perpetúe su poder, mientras que la población se enfrenta a la desinformación y a la represión.



QARMAS

1. ¿De qué forma pueden las armas cibernéticas ser utilizadas para interferir en los procesos electorales, y qué implicaciones tiene esto para la integridad nacional?
2. ¿Qué acciones pueden tomar los gobiernos para salvaguardar sus sistemas electorales de ataques cibernéticos?
3. ¿Cómo influyen las armas cibernéticas en las relaciones diplomáticas entre países, especialmente en el espionaje y las inteligencias?
4. ¿De qué forma el ciber espionaje impacta la confianza entre naciones y la estabilidad política a nivel internacional?
5. ¿Cómo pueden las armas cibernéticas amenazar la soberanía de un Estado, y cuáles son los retos para la defensa nacional en el ciberespacio?
6. ¿Cómo se define un acto de guerra cibernética, y qué tipo de respuesta sería considerada proporcional y moral?
7. ¿Cómo se emplean las armas cibernéticas para propagar desinformación y propaganda, y cuáles son sus efectos en la opinión pública y la estabilidad política?
8. ¿Qué papel juegan las redes sociales en la difusión de información falsa y manipulada?
9. ¿Cómo impacta el uso de armas cibernéticas en las relaciones internacionales?
10. ¿Qué tipo de acuerdos internacionales podrían establecerse para regular el uso de armas cibernéticas?
11. ¿Cómo pueden los ataques cibernéticos a infraestructuras críticas (salud, energía, agua) afectar la vida diaria de las personas?
12. ¿De qué manera pueden las armas cibernéticas infringir la privacidad y los derechos humanos de los ciudadanos?



MATRIZ DISEC

Alemania	Israel
Arabia Saudita	Italia
Australia	Japón
Brasil	México
Canadá	Noruega
China	Omán
Corea del Norte	Países Bajos
Corea del Sur	Pakistán
Dinamarca	Reino Unido
España	Rumania
Estados Unidos	Rusia
Finlandia	Singapur
Francia	Suecia
India	Turquía
Irán	Ucrania

Referencias

- Access Now.* (2021). *La vigilancia digital: cómo las fuerzas de seguridad utilizan datos para arrestar manifestantes.* <https://www.accessnow.org/security-forces-arrests>
- Asamblea General de las Naciones Unidas (s.f.).* Primera Comisión (Desarme y Seguridad Internacional). <https://www.un.org/es/ga/first/index.shtml>
- Barracuda Networks.* (2023). *The dawn of real-time defense: Security transformation in the 2000s.* <https://blog.barracuda.com/2023/11/28/the-dawn-of-real-time-defense-security-transformation-in-the-2000s>
- Bloxberg, D.* (2024). *20 Years of Cyber Security Awareness: Evolution of Security.* VIPRE Security Group. <https://inspiredelearning.com/blog/20-years-cyber-security-awareness>
- Centro de Análisis de Políticas Europeas (CEPA).* (2020). *Rusia y los ciberataques: una extensión de su política militar.* <https://www.cepa.org/russian-cyber-attacks>
- Cybersecurity & Infrastructure Security Agency.* (2021). *Ciberataques en elecciones: estadísticas y análisis.* <https://www.cisa.gov/election-cyber-attacks>
- Human Rights Watch.* (2021). *Tecnología y represión: la libertad de expresión bajo amenaza.* <https://www.hrw.org/technology-repression>
- ManageEngine* (2025). *Infografía: Evolución de la ciberseguridad. Historia de la ciberseguridad.* <https://www.manageengine.com/latam/log-management/infografia-evolucion-ciberseguridad.html>
- Misión Permanente de México ante la Organización de las Naciones Unidas (s.f.).* Primera Comisión. <https://mision.sre.gob.mx/onu/index.php/at/primera-comision>
- MUNUC.* (s.f.). DISEC 37. <https://munuc.org/committees/dise-37/>
- North American Invitational Model United Nations (NAIMUN).* (s.f.). DISEC. <https://naimun.modelun.org/dise-37>
- Organización del Tratado del Atlántico Norte (OTAN).* (2020). *Ciberamenazas: la percepción de los miembros de la OTAN sobre la seguridad nacional.* <https://www.nato.int/cyber-threats>
- Organización del Tratado del Atlántico Norte (OTAN).* (2021). *Desafíos constantes: armas cibernéticas y la necesidad de cooperación internacional.* <https://www.nato.int/cyber-weapons-security>



Organización del Tratado del Atlántico Norte (OTAN). (2021). Operaciones de influencia rusa: socavando la confianza en el gobierno ucraniano.
<https://www.nato.int/influence-ukraine>

Prieto (2025). ¿Cuál es la historia de la ciberseguridad?. Saint Leo University.
<https://worldcampus.saintleo.edu/blog/historia-de-la-ciberseguridad>

PW_ Guía de comisión DISEC 1. (s.f.). Secretaría de Educación del Distrito.
https://www.educacionbogota.edu.co/portal_institucional/sites/default/files/inlin_e-files/PW_Gu%C3%ADa%20de%20comisi%C3%B3n%20DISEC%201.pdf

Reaching Critical Will. (s.f.). UN General Assembly (UNGA).
<https://www.reachingcriticalwill.org/disarmament-fora/unga>

Stuxnet. El Primer Ciberarma de la Historia #CortoDocumentales