APROXIMACIÓN A LOS CIBERATAQUES DESDE LOS DERECHOS HUMANOS

LAURA DANIELA HERNÁNDEZ NARVÁEZ
CAMILA ANDREA ORTIZ MÉNDEZ

UNIVERSIDAD SANTO TOMÁS
FACULTAD DE DERECHO
MAESTRÍA EN DERECHOS HUMANOS
VILLAVICENCIO
2024

APROXIMACIÓN A LOS CIBERATAQUES DESDE LOS DERECHOS HUMANOS

LAURA DANIELA HERNÁNDEZ NARVÁEZ
CAMILA ANDREA ORTIZ MÉNDEZ

Artículo académico presentado como requisito para optar al título de Magister en Derechos Humanos

Asesor
Mg. RODRIGO CORTÉS BORRERO
Magíster en Derecho contractual público y privado

UNIVERSIDAD SANTO TOMÁS
FACULTAD DE DERECHO
MAESTRÍA EN DERECHOS HUMANOS
VILLAVICENCIO
2024

Autoridades Académicas

P. Álvaro José ARANGO RESTREPO, O. P.
Rector General

P. Mauricio Antonio CORTÉS GALLEGO, O. P.
Vicerrector Académico General

P. José Antonio BALAGUERA CEPEDA, O. P.
Rector Seccional Villavicencio

P. Rodrigo GARCIA JARA, O. P.
Vicerrector Académico Seccional Villavicencio

Mg. JULIETH ANDREA SIERRA TOBÓN
Secretaria General Seccional Villavicencio

Mg. RODRIGO CORTÉS BORRERO
Decano de la Facultad de Derecho

Aproximación a los ciberataques desde los Derechos Humanos

Laura Daniela Hernández Narváez[1]

Camila Andrea Ortiz Méndez[2]

Resumen

El presente artículo aborda la necesidad de realizar una aproximación descriptiva sobre los ciberataques desde una perspectiva de derechos humanos, con la aplicación del enfoque teórico y método descriptivo, se vislumbraron conceptos sobre el ciberataque y sus tipos. Con ello se permitió recopilar datos detallados y objetivos sobre el ataque cibernético, identificar patrones y características, presentar los hallazgos de manera objetiva con el análisis de cuatro ciberataques alrededor del mundo. Por ello, las autoras analizan que en cualquier lugar en la cual la persona traslade su vida, los derechos humanos se trasladan con él, para demostrar que no hay regulación específica para los ataques realizados en el ciberespacio y con ello determinar que es necesario ampliar la normativa vigente para proteger más efectivamente los derechos humanos.

Palabras Clave: Ciberespacio, Derechos Humanos, Ciberataque, Ciberseguridad, Avances Tecnológicos.

Abstract

This article addresses the need to carry out a descriptive approach to cyberattacks from a human rights perspective, with the application of the theoretical approach and descriptive method, concepts on cyberattacks and their types were glimpsed. This made it possible to collect detailed

[1] Abogada graduada de la Universidad Santo Tomás en el año 2022. Conciliadora en Derecho. Especializada en Defensa de los DDHH de la Universidad Santo Tomás. Se ha desempeñado como coordinadora jurídica de instituciones privadas y prestadora de servicios en entidades territoriales.

[2] Abogada graduada de la Universidad Santo Tomás en el año 2016. Conciliadora en Derecho. Especializada en Derecho Administrativo y Magíster en Derecho Administrativo de la Universidad Santo Tomás. Se ha desempeñado como auxiliar jurídico y prestadora de servicios ante la Procuraduría General de la Nación y Personerías Municipales, abogada litigante ante la jurisdicción de lo Contencioso Administrativo y asesora jurídica de entidades públicas y privadas. Trabaja como docente universitaria de pregrado y posgrado desde el año 2022.

and objective data on the cyber attack, identify patterns and characteristics, and present the findings objectively with the analysis of four cyber attacks around the world. Therefore, the authors analyze that wherever a person relocates their life, human rights relocate with them, to demonstrate that there is no specific regulation for cyberattacks and thereby determine the necessity to expand current legislation to more effectively protect human rights.

Key Word: Cyberspace, Human Rights, Cyberattack, Cybersecurity, Technological Advances.

Introducción

El ser humano es atraído por el poder y así satisface su necesidad de dominio, en ocasiones, a través de la violencia, violencia que lleva a una clara vulneración de derechos humanos. En el análisis de las diferentes expresiones de poder, José Marina encuentra dos elementos antitéticos: seducir y aterrorizar. El temor se relaciona con el ejercicio de poder, el temor que debe impartirse a los súbditos para con ellos mantenerlos subordinados en un estado de inseguridad e intranquilidad. La intranquilidad provoca más vulnerables a los dominados, sin embargo, en ocasiones, el miedo crea reacciones de defensa (Lutz, 2012).

En estos ejercicios de poder y generación de conflictos pueden verse inmiscuidas intenciones concretas sobre dominar territorio, población o recursos naturales, como también estar relacionados a temas políticos o religiosos. Ahora bien, con los avances tecnológicos también han avanzado esas intenciones del ser humano de demostrar poder en otros escenarios, como lo es en el ciberespacio.

Desde 1903, cuando el primer *hacker*, el británico John Nevil Maskelyne, quien era a su vez un ilusionista/mago, interceptó la demostración pública del telégrafo inalámbrico de Giuliano Marconi (Chipana Luna, 2013) a la fecha, se han realizado miles de ciberataques por razones diversas, lo que también podría decantar en violaciones directas e indirectas a derechos humanos. Cuando la vida del ser humano se traslada al ciberespacio, sus derechos se trasladan junto a él, al ser inherentes.

Con este nuevo panorama de desarrollos tecnológicos y digitales es imprescindible plantear el problema de sí ¿Es factible vulnerar derechos humanos a través de ciberataques en el ciberespacio? En este contexto, el presente artículo tiene como objetivo brindar una aproximación

descriptiva sobre los ciberataques desde una perspectiva de derechos humanos, reconociendo los casos en los que se han presentado ciberataques y con ello, identificar las posibles vulneraciones a los derechos humanos en el ciberespacio.

1. Un acercamiento al concepto de ciberataque

Cuando se analizan los impactos generados por los avances tecnológicos, es imperativo realizarlo con cautela. Por un lado, se puede evocar a la mejoría de la calidad de vida en múltiples campos, como son la medicina, seguridad alimentaria, educación, redes de telecomunicaciones, transporte, agroindustria, etc… lo que ha permitido el mejoramiento en la calidad de vida a muchas personas; por ejemplo, con la creación de la Internet, se ha revolucionado completamente el acceso a la información y comunicación, permitiendo la expansión y conectividad global.

Sin embargo, dentro del análisis también se encuentran desafíos, que a su vez han tenido un impacto significativo en la sociedad; la creación de armas nucleares y/o biológicas, nuevas desigualdades, modificación de virus y enfermedades a través de ingeniería genética, desempleo tecnológico, *fake news, etc…* lo que ha conllevado en que la misma red que ha revolucionado completamente la sociedad puede ser utilizada para amenazar la seguridad cibernética y generar violación a derechos humanos.

Empero, independientemente del uso del avance tecnológico se pueden desprender amenazas que pueden provenir de actores no estatales o desde las instituciones y empresas que usan la tecnología como un vector de control y poder. Estas luchas transforman la sociedad, modelos políticos, estructuras tecnológicas, sistemas económicos y culturales, generando altercados por medio de estas dinámicas de dominación, realizando no sólo ataques físicos sino también digitales (Crespo, 2020).

Es por ello que, es menester conocer los conceptos generales que se ven inmiscuidos en estas dinámicas de control y poder, como lo son el ciberespacio, ciberataque, ciberseguridad, ciberdefensa e infraestructura crítica.

1.1. Qué es el ciberespacio

Aunque el concepto de ciberespacio ha cobrado una importancia monumental en la era moderna, su origen se remonta a literatura de ciencia ficción de 1984, pues, el término fue acuñado por primera vez por el escritor William Gibson en su novela "Neuromante", donde expone que el ciberespacio es: "*una representación gráfica de información abstraída de los bancos de todos los ordenadores del sistema humano. Una complejidad inimaginable. Líneas de luz clasificadas en el no–espacio de la mente, conglomerados y constelaciones de información*". (Gibson, 2006, p. 26)

A pesar de su origen ficticio, el ciberespacio ha trascendido el texto literario para convertirse en una realidad palpable en la sociedad actual, influyendo en todos los aspectos de la vida cotidiana, desde la manera en la que las personas interactúan, trabajan y hasta en cómo se accede a la información; bien lo dijo Castells (2001), "*el ciberespacio ha transformado la manera en que interactuamos socialmente, creando nuevas formas de comunicación y comunidades virtuales*" (p. 15).

Pero, pese a sus innumerables beneficios, el ciberespacio también se presenta como un desafío significativo en la protección de los derechos humanos, pues, en la actualidad, el ciberespacio se ha convertido en un nuevo campo de batalla donde pueden ocurrir ciberataques, dejando de lado los espacios tradicionales de los enfrentamientos armados, bien lo manifestó Ayala (2019):

Ese mundo físico, usualmente está constituido por los llamados "dominios", esto es, la tierra, el mar, el aire y el espacio. Sin embargo, la idea del ciberespacio como un escenario donde se desarrollan conflictos armados ha suscitado una serie de discusiones en los últimos años en torno a si se trata de un espacio semejante a los demás ya conocidos o, por el contrario, debe tratarse con pinzas y de un modo especial por las características que lo identifican. De ahí que exista un variado número de pensadores e instituciones, quienes opinan que el ciberespacio es un ambiente perteneciente al mundo físico y, por consiguiente, digno de ser llamado "quinto dominio" o "quinta dimensión de la guerra". (párr. 8)

1.2. Qué es un ciberataque o ataque cibernético

Con el creciente uso de la tecnología en todos los aspectos de la vida moderna, los ciberataques se han convertido en una amenaza significativa tanto para organizaciones, gobiernos e individuos, por lo que Sigholm (2014) afirmó lo siguiente:

Los ataques cibernéticos son un subconjunto de las operaciones ciberespaciales donde se emplean las capacidades hostiles del ciberespacio por parte de Estados o actores no estatales para causar daño, destrucción o bajas a fin de lograr objetivos militares o políticos. (p. 6)

Es decir, que si partimos de la idea primigenia del concepto de “ataque” como aquel acto de inducir a la destrucción, perjuicio, daño, menoscabo ya sean a bienes o servicios, infraestructuras, a organizaciones particulares, gubernamentales o instituciones estatales, lo que podemos inferir es que el ciberataque puede regirse bajo los mismo verbos rectores con la diferencia de que este se origina y se desarrolla en el ciberespacio y que el objetivo del ataque será encontrado en el mundo virtual.

Así mismo, la actividad hostil en el ciberespacio puede clasificarse según los tipos de actividad realizada y el daño causado, como lo manifiesta Tabansky (2011):

> a. Un ataque a diversos objetivos civiles que cause daño físico.
>
> b. La interrupción y el ataque a infraestructuras críticas de información nacional, que cause daño físico.
>
> c. La interrupción y el ataque a objetivos militares en el territorio soberano del Estado.
>
> d. La interrupción y el ataque a objetivos militares fuera del territorio soberano del Estado.
>
> e. La inserción de herramientas de ataque latentes, por ejemplo, un caballo de Troya o una bomba lógica, que probablemente sean preparativos para un ataque.
>
> f. Actividad criminal, espionaje industrial.
>
> g. Uso de armas de doble uso: recopilación de inteligencia, sondeo de vulnerabilidades de seguridad comunes, pruebas de penetración.
>
> h. Realización de una campaña de propaganda mediática, abuso y desfiguración de sitios web oficiales. (p. 82)

Por otro lado, cabe resaltar que a pesar de que, en la cotidianidad, el uso de la palabra se hace sin distinción, y se usa en un marco militar, estratégico y estatal, es un error pensar que solo se usa en esos ámbitos, ya que los ciberataques no son ajenos al sector privado y particular.

1.2.1 Motivos

En la era digital, los ciberataques se han convertido en una amenaza omnipresente, impulsados por diversas motivaciones que reflejan la complejidad de la sociedad moderna; estos ataques pueden ser motivados por razones criminales, personales y políticas, cada una con sus propias dinámicas y objetivos.

Es así como los atacantes con motivaciones delictivas buscan obtener ganancias financieras mediante el robo de dinero, el robo de datos o la interrupción del negocio, por lo que los ciberdelincuentes pueden piratear una cuenta bancaria para robar dinero directamente o utilizar estafas de ingeniería social para engañar a las personas para que les envíen dinero. Los piratas informáticos pueden robar datos y utilizarlos para cometer robos de identidad o venderlos en la Dark Web o guardarlos para un rescate; por otro lado, los agresores con motivaciones personales, como los empleados actuales o antiguos, buscan principalmente la retribución por algún desaire percibido, por lo que pueden tomar dinero, robar datos confidenciales o interrumpir los sistemas de una empresa; y finalmente, los atacantes con motivaciones políticas suelen asociarse con la guerra cibernética, el ciberterrorismo o el "hacktivismo". En la ciberguerra, los actores de los estados-nación suelen atacar las agencias gubernamentales o la infraestructura crítica de sus enemigos. (International Business Machines Corporation, s.f).

Hablar de los motivos de los ciberataques es crucial ya que permite a las organizaciones y a los gobiernos desarrollar estrategias de ciberseguridad y ciberdefensa más efectiva y específicas, así mismo, ayuda a identificar y clasificar las amenazas de manera adecuada y por consiguiente buscar la respuesta proporcional, además, abordar los motivos de los ciberataques contribuye a una mayor concienciación y educación sobre los riesgos en el ciberespacio

Así mismo, al conocer las motivaciones para realizar los ciberataques, se hace de vital importancia conocer los conceptos de ciberseguridad y ciberdefensa, ya que son términos que a menudo son utilizados sin distinción alguna, pero que en realidad tienen enfoques y alcances diferentes, por un lado, la ciberseguridad se centra en la implementación de medidas preventivas,

defensivas y reactivas para proteger los sistemas de información y los datos contra una amplia gama de amenazas, en cambio, la ciberdefensa se orienta específicamente hacia la protección activa y la respuesta a ataques dirigidos contra infraestructuras críticas, con un enfoque estratégico y militar. A continuación, se desarrollan ambos conceptos:

1.3. Qué es la ciberseguridad

En el contexto actual, los ciberataques representan una amenaza creciente para los derechos humanos, desafiando las normativas legales y éticas establecidas. Deibert (2020) argumenta que "*la seguridad cibernética es crucial para la preservación de la sociedad civil*" (p. 112), enfatizando la necesidad de regulaciones efectivas que protejan los derechos individuales en un entorno digital cada vez más complejo.

En ese sentido, la ciberseguridad tiene como objetivo proteger los sistemas, las aplicaciones, los dispositivos informáticos, los datos confidenciales y los activos financieros de las personas y las organizaciones contra virus informáticos, ataques de ransomware sofisticados y costosos, entre otros, y teniendo en cuenta que las tendencias en expansión de la tecnología de la información de los últimos años incluyen: 1) un aumento de la adopción de la computación en la nube, 2) complejidad de la red, 3) trabajo remoto y trabajo desde casa, 4) programas bring your own device (BYOD), 5) dispositivos y sensores conectados en todo, desde timbres hasta automóviles y líneas de ensamblaje, por lo que todas estas tendencias crean enormes ventajas comerciales y progreso humano, pero también brindan exponencialmente más oportunidades para que los delincuentes cibernéticos ataquen. (International Business Machines Corporation, s.f)

1.4. Qué es la ciberdefensa

En la era digital moderna, la protección de infraestructuras críticas y sistemas de información ha adquirido una importancia sin precedentes, aunado a esto, la creciente dependencia de la tecnología para funciones esenciales, ha hecho que los ciberataques sean una amenaza cada vez más significativa. En este contexto, Vargas et al. (2017), manifiesta que la ciberdefensa es:

> las acciones de un Estado para proteger y controlar las amenazas, peligros o riesgos de naturaleza cibernética, con el fin de permitir el uso del ciberespacio con normalidad, bajo la protección de los derechos, libertades y garantías de los ciudadanos, en apoyo a la defensa de la soberanía y la integridad territorial; sin soslayar que en los nuevos escenarios que plantea el ciberespacio, pueden incidir en el momento de trazar rutas estratégicas plausibles para el cumplimiento de las diversas misiones militares de ciberdefensa. (p. 32)

1.5. Infraestructura de información crítica

En un mundo cada vez más interconectado y dependiente de la tecnología, el concepto de "infraestructura crítica" se constituye como la columna vertebral de cualquier sociedad moderna, abarcando los sistemas y activos esenciales para el funcionamiento continuo de servicios vitales como la energía, el agua, las telecomunicaciones, el transporte y la salud pública, es por esta razón que es de vital importancia proteger estos componentes.

Por otro lado, se ha manifestado que las infraestructuras críticas son:

> Las infraestructuras críticas son aquellas sin las que una sociedad no puede mantener el ritmo de vida que ha mantenido con anterioridad. Son las que se mantienen, protegen y supervisan con márgenes de seguridad amplios para que siempre se pueda contrarrestar cualquier tipo de situación complicada. Siempre son estructuras que están sobre-protegidas (Universidad Internacional de Valencia, s.f.).

Teniendo en cuenta lo mencionado anteriormente, se puede inferir que los blancos predilectos de los ciberataques son precisamente la infraestructura crítica debido a su importancia estratégica y su impacto directo en la estabilidad y seguridad de un estado, ya que los ciberataques dirigidos a la infraestructura crítica pueden provocar interrupciones en servicios esenciales generando caos y debilitando la capacidad de respuesta de una sociedad ante emergencias; es por esto, que la infraestructura crítica se han convertido en prioridades estratégicas para los gobiernos y organizaciones a nivel global.

Es importante señalar que la definición de infraestructura crítica puede variar entre estados, ya que depende de las características e intereses particulares de cada uno, aunque no

existe un consenso claro sobre cuáles son exactamente estas infraestructuras, generalmente tienden a ser similares en la mayoría de los casos (Ayala, 2019).

En conclusión, abordar las categorías de ciberseguridad, ciberespacio, ciberataque, ciberdefensa, los motivos detrás de estos actos y la protección de la infraestructura crítica es esencial para dar inicio al desarrollo de la investigación; a modo de resumen se puede decir que la ciberseguridad se erige como la primera línea de defensa en el ciberespacio, un ámbito vasto y complejo que conecta a nivel global, pero que también es vulnerable a ciberataques y que estos pueden tener motivaciones diversas, desde el ámbito político, personal y delictivo, lo que resalta la necesidad de estrategias de ciberdefensa robustas, además, la protección de la infraestructura crítica, que incluye sectores como la energía, el agua, las telecomunicaciones y el transporte, es vital para prevenir interrupciones que podrían tener consecuencias catastróficas.

2. Tipos de ataques cibernéticos

Los enfrentamientos armados han sido una presencia constante en la historia humana, emergiendo como un mecanismo esencial en la búsqueda de metas de poder. Estos conflictos han experimentado una evolución continua, adaptándose a las demandas particulares de cada situación: la irrupción de nuevos protagonistas armados, los avances tecnológicos y las mutaciones en las estrategias de batalla (Ayala, 2019).

En ese contexto, teniendo claridad que conforme a los avances tecnológicos y a las nuevas estrategias de batalla es posible realizar ataques en el ciberespacio que afecten a instituciones o personas con el objetivo de captar información, adulterarla, destruirla, espiar o manipular, y en el entendido que la presencia de enfrentamientos es un constante en la existencia humana, se puede inferir que los ciberataques serán habituales y por ello, en aumento. Respecto al ciberataque, se puede indicar que es un asalto realizado por criminales o ciberdelincuentes con el fin de deshabilitar ordenadores de forma maliciosa, robar, secuestrar datos o usar dispositivos contaminados como punto de lanzamiento para otras amenazas (García Bordonado, 2022, p. 6).

Con la intención de demostrar poder y control existen actualmente varios tipos de ciberataques, y en el entendido que:

> El principal motivo de infección de los sistemas informáticos es causado por el usuario, quien ejecuta el virus y permite la instalación sin saberlo; en segundo

> lugar, están los gusanos que infectan el sistema informático donde se encuentra y se replican a través de la red. (Garcia, 2017, pp 4)

Por lo anterior, es importante profundizar en el Malware o software malintencionado y sus respectivos tipos y/o clasificación, en consecuencia, se exponen a continuación:

2.1. Malware o Software malintencionado

El malware es una palabra que se origina de la combinación de dos términos en inglés *Malicious* y *Software*, la cual traduce Software malicioso. El malware, son aplicaciones malintencionadas creadas con el objetivo de dañar o alterar dispositivos físicos que se conectan a un sistema de red sin el consentimiento del usuario.

Cronológicamente, respecto al el primer Malware se podría mencionar que:

> En 1971, Robert Thomas, de la compañía BBN, creó *Creeper*, un programa que se movía entre ordenadores conectados a ARPANET y que desplegaba el mensaje "*I'm the creeper: catch me if you can*". Según resume a OpenMind David Harley, consultor de seguridad informática e investigador para la compañía ESET, "en la comunidad investigadora solemos considerar el programa experimental *Creeper* como el primer virus y/o gusano". (Yanes, 2023, párr 5)

Con los avances tecnológicos, también los Malware fueron avanzando y a través del engaño alterando dispositivos de punto de conexión y dependiendo de su comportamiento, dichos Software maliciosos pueden clasificarse como adware, spyware, troyanos, gusanos, ransomware, entre otros. En ese sentido, se van a realizar el análisis de los cuatro tipos más habituales:

2.1.1 Virus

El virus, es el software malintencionado más habitual y conocido, como su nombre lo indica es un malware infeccioso que se adhiere a programas y se replica, generando la modificación y destrucción de archivos, sin embargo, para su activación y propagación se requiere la ejecución de la aplicación infectada.

Según la multinacional tecnológica estadounidense, Microsoft Corporation (s.f), "*Los virus están diseñados para interferir en el funcionamiento normal del dispositivo y registrar*,

dañar y eliminar sus datos. Suelen engañar a los usuarios para que abran archivos malintencionados y, de esta manera, se propagan a otros dispositivos".

En ese sentido, éste malware requiere para cumplir su finalidad infecciosa y su supervivencia, la interacción directa humana.

2.1.2 Gusano

A diferencia de los virus, la finalidad de los gusanos no es infectar archivos, es propagarse en el mayor número de dispositivos y colapsarlos, aprovechando su característica de autosuficiencia que significa que pueden propagarse sin interacción del usuario, incluso con los dispositivos apagados aprovechándose de las vulnerabilidades de la red para propagarse.

Este malware suele utilizar tácticas de ingeniería social para maximizar su efectividad. Para cumplir esta finalidad, los creadores de malware eligen nombres o temas atractivos para ocultar el archivo malicioso, los cuales se propagan al enviar archivos adjuntos infectados a otros usuarios a través de correos electrónicos, mensajes instantáneos, etc. De manera inadvertida, los usuarios receptores descargan y abren dichos archivos, contribuyendo así a la propagación del virus (Panda a WatchGuard brand, s.f).

2.1.3 Ransomware

Es un tipo de software malicioso que secuestra y amenaza con destruir o bloquear el acceso a información del usuario, todo lo realiza con la finalidad de que la víctima pague un rescate.

Según Microsoft Corporation (s.f), los ataques de Ransomware son usualmente dirigidos a grandes organizaciones, ya que pueden solicitarles un pago económico más elevado, dado el riesgo de filtrar información confidencial o sufrir ataques adicionales de ciberdelincuentes, el método habitual para acceder a la red de la organización, es el robo de credenciales de un empleado real para hacerse pasar por esa persona y acceder a sus cuentas para ello usan configuraciones erróneas de seguridad para infiltrarse, recorrer su red empresarial y adaptarse al entorno y a cualquier debilidad.

Estos ataques van en aumento y con ello su actuar se torna más organizado, muchas de las operaciones de ransomware implican la intervención de varios delincuentes.

2.1.4 Phishing o Suplantación de identidad

Una técnica de ciberdelincuencia donde el engaño y fraude predomina al poder lograr el robo de información personal y financiera de la víctima. En el phishing o suplantación de identidad, el ciberdelincuente se hace pasar por una fuente confiable lo que genera que la víctima sin ninguna sospecha, ingrese sus datos confidenciales a través de sitios web, correos electrónicos o mensajes de datos culminando con el robo de su información, identidad o de dinero de directamente sus cuentas bancarias. Se puede determinar que el objetivo es:

> recolectar información de autenticación de sitios web del usuario (información de bancos, cuentas de correo, redes sociales, entre otros); a través de un archivo ejecutable o un enlace enviado vía correo electrónico, el usuario es direccionado a un sitio web falso, diseñado para que el usuario sienta que ingresa al sitio web legítimo e ingrese su información confidencial de acceso (usuario, contraseña, entre otros). (Garcia, 2017, pp 3)

Se determina con lo anterior que, estos software malintencionados usados por los ciberdelincuentes con el objetivo de infectar, destruir o causar daños a dispositivos o servidores impactan de forma negativa el desarrollo de los servicios, instalaciones y recursos, con el avance a la era digital y el creciente uso de los sistemas informáticos ha permitido que los ciberdelincuentes se sientan más atraídos a atacar las vulneraciones de las tecnología mediante las prácticas maliciosas con la intención de obtener un beneficio propio o con el simple hecho de generar daños.

3. Escenarios reales de violación de DDHH a través de ciberataques

En la historia existen importantes escenarios donde los ataques en el ciberespacio han implicado un antes y un después en transformaciones estructurales en ciberdefensa y ciberseguridad en Estados, organizaciones y particulares.

Para realizar un análisis global y hablar de algunos de los primeros e importantes ciberataques realizados que generaron daños a infraestructura física o entorpecieron el acceso a servicios esenciales, se destacan cuatro ciberataques que se desarrollaron a través de Malwares tipo Gusano y Ransomware en los continentes de Asia, Europa y América.

3.1. Stuxnet (2010)

En 2010, se dió por primera vez un ataque cibernético que generó daños materiales a infraestructura física en una planta de enriquecimiento de uranio en Natanz, Irán; estos daños fueron generados por un sofisticado programa malicioso, un "gusano" ahora conocido como *Stuxnet.*

Con sofisticación tecnológica, el "gusano" aprovechó cuatro debilidades desconocidas por el sistema operativo Windows de Microsoft y generó de manera anónima y devastadora daños a aproximadamente a 1.000 centrífugas, Stuxnet penetró en la red del programa nuclear de Natanz de Irán en una memoria USB infectada que fue insertada en una computadora conectada al sistema informático de la planta; lo que llevó a que se propagara al software que controlaba las centrifugadoras y se insertó en él, tomando el control de dichas máquinas fundamentales para aislar el uranio enriquecido. Estos ataques fueron realizados en distintas ocasiones, por meses. Lo que conllevó, que, con el tiempo, la tensión provocada por la aceleración y desaceleración sin control causará que las máquinas infectadas se desintegraron (BBC, 2015).

Aunque, según Rivadeneira (2016), se realizaron investigaciones, nunca se ha revelado oficialmente quién o quiénes crearon a Stuxnet, sin embargo, se cree que fue desarrollado por los gobiernos de Estados Unidos e Israel como respuesta a su preocupación por el progreso acelerado de Irán en su programa de armas nucleares. Incluso, de manera no oficial se conoció que esta "estrategia alternativa" para retrasar los planes de Irán, fue supuestamente denominada "Operación Juegos Olímpicos" la cual constituyó el primer empleo del ciberespacio como un campo de batalla con ciberarmas (pp. 78).

A la fecha, no existe consenso respecto a las consecuencias del ataque de Stuxnet. En el escenario geopolítico se ha indicado, incluso que:

Por una parte, su acción disuadió a Israel de un ataque aéreo sobre Irán, también retrasó el programa iraní al menos de seis meses a dos años, ganando tiempo para que se impusiese la diplomacia. No evitó, en cambio, el progreso armamentístico nuclear por parte de Irán, ya que este se vio asediado políticamente y su orgullo le hizo autoconvencerse de que tenía que hacer frente a esta nueva guerra digital y culminar sus planes nucleares. Un problema político quiso afrontarse con instrumentos técnicos. (Romero, 2022, párr 27)

Con este primer ataque cibernético, se demostró que las ciberarmas existen y pueden llegar a producir efectos militares similares al armamento convencional.

3.2. BlackEnergy (2015)

Según Aucal Business School (2016) el ataque fugaz y sin precedentes se llevó a cabo en Ucrania en diciembre de 2015, donde por primera vez se usó un programa malicioso llamado BlackEnergy para realizar un apagón eléctrico generalizado al infiltrarse en el sistema de tres compañías energéticas y cerrar temporalmente la generación de energía en tres regiones ucranianas, cabe mencionar aparentemente el programa malicioso distribuyó mediante correos electrónicos de *spear phishing*, es decir, correos personalizados con adjuntos de Microsoft Office maliciosos.

Aproximadamente 225.000 personas quedaron sin electricidad por casi seis horas en pleno invierno. Los cibercriminales con el fin de dificultar las magnitudes del ataque, fueron más allá y decidieron bloquear todas las comunicaciones tanto telefónicas como por web entre el sistema de control y entre los clientes.

Por el análisis que se realizó posterior al ataque, se pudo inferir que:

> Un empleado de una central eléctrica de Ucrania recibió un mensaje de correo electrónico que le animaba a pinchar en un documento adjunto. Al hacerlo, se instaló un código malicioso en su ordenador, que lo conectó al ordenador de los criminales y abrió una puerta trasera. Por esta puerta entró BlackEnergy, un virus del tipo troyano que se instaló en tantos ordenadores como pudo y allí se quedó, en silencio, espiando los movimientos en la central. En un momento dado, los atacantes instalaron a distancia un nuevo módulo a BlackEnergy, llamado KillDisk. KillDisk está programado para destruir archivos vitales de los ordenadores de una central eléctrica. Después manipularon remotamente los ordenadores para provocar los apagones y, acabado el trabajo, activaron KillDisk, que destruyó los discos duros borrando así las huellas de los hackers en el sistema. (Molist, 2016, párr 5)

Igual que en el caso de Stuxnet, no se han confirmado los involucrados en el hackeo de esta infraestructura crítica, pero el gobierno de Ucrania responsabilizó a Rusia, por usar el

componente destructivo KillDisk el cual borró archivos de sistema y corrompió el master boot record (MBR), dejando a los sistemas inutilizados generando vulneración a los derechos de los clientes de las empresas de servicios públicos en el oeste de Ucrania.

3.3. Ransomware (2021)

Colonial Pipeline, es una empresa que controla la red de oleoductos que suministran combustible como gasolina y diésel a una gran parte de la costa este y sur de los Estados Unidos, desde Texas hasta New Jersey, puede transportar alrededor de tres millones de barriles de combustible; es por ello que al dar servicio a la mayoría de los estados del sur y tener ramificaciones de la costa Atlántica, el ataque cibernético que le realizaron en mayo de 2021, desencadenó el pánico en las gasolineras y ciudadanos del país (New York Times, s.f).

Así mismo, según Rockwell Automation (s.f) El ataque se originó con un ransomware, que es un código malicioso que tomó el control de las computadoras del entorno de la tecnología de la información (TI) de la compañía estadounidense, pero dicho ataque no impactó sólo a la empresa, a la vez afectó a otros negocios de la cadena de suministro de combustible, consumidores, y por supuesto, al gobierno de Estados Unidos.

Se pudo determinar que no fue un ataque cualquiera con la intención de sólo afectar el acceso a gasolina y diésel, contrario a lo sucedido en Irán y Ucrania, se pudo determinar quién realizó el ataque. El grupo DarkSide, sindicado como autor del perjuicio, es calificado como una pandilla criminal que intimida, bloquea y roba datos mediante cifrado y amenaza con liberarlos a menos que se pague un rescate. Cinco días antes de anunciar que el sistema estaba encriptado, a la empresa le extrajeron aproximadamente 100 GB de datos de red corporativa, según la investigación se puede sugerir que probablemente un empleado de la compañía usó la credencial empresarial en otra cuenta que fue hackeada.

Según la BBC (2022), los autores del ataque, no son hackers rusos como se pensaba inicialmente, pero se cree que tienen su base de operaciones en Rusia. Con la intimidación, la empresa del gasoducto admitió haberles pagado a los criminales US$4,4 millones en bitcoins, difíciles de rastrear, a cambio de volver a poner en funcionamiento los sistemas informáticos. Como consecuencia del ataque, se disparó en el país estadounidense el coste de la gasolina en un 4%.

3.4. Ransomware (2022)

Según el Tiempo (2022), Keralty es un proveedor de atención médica que opera a través de hospitales y centros médicos en América Latina, España, Estados Unidos y Asia. En Colombia, el grupo Keralty ofrece servicios de salud a través de sus subsidiarias, la EPS Sanitas y su servicio de medicina prepagada, Colsanitas.

En noviembre de 2022, más de 5.500 colombianos y colombianas afiliados a la EPS Sanitas o con servicios de medicina prepagada de Colsanitas, se vieron afectados por una violación de la información en sus historiales clínicos y el acceso a servicios de salud producto del ciberataque dirigido a la organización multinacional Keralty, impidiéndoles a los afectados, el acceso a servicios de salud, fallas en la asignación de citas, entrega de medicamentos y exámenes, entre otros.

El grupo de hackers, RansomHouse se atribuyó la responsabilidad por el hackeo que afectaron los sitios web y operaciones de la empresa y sus subsidiarias, los autores del perjuicio pidieron un rescate luego de extraer la información confidencial y siguieron amenazando la privacidad de los datos obtenidos.

Posterior al ciberataque, MuchoHacker.lol (2022) pudo lograr contactar a RansomHouse que luego de increparles si sabían que este tipo de actos podían afectar la vida de cientos de personas, incluso de bajos recursos, indicaron:

> Quizás usted tenga que hacerle esta pregunta a la empresa afectada. Usted debería preguntarles a ellos por qué ponen en riesgo a sus clientes por cuenta de fallas en sus sistemas de seguridad. Ponen por encima los beneficios económicos que la protección de datos. Nosotros estamos negociando. Nosotros no encriptamos, estamos intentado buscar una solución entre las partes de tal manera que todo los involucrados permanezcan indestructibles. Creo que la pregunta se la deben hacer a Keralty. El paquete de evidencias estará disponible en nuestro sitio web en los próximos días. (Párr 5)

En estos cuatro escenarios reales analizados, se pudo determinar que independientemente del Estado donde se realizaron los ciberataques, todos fueron realizados a infraestructuras críticas, como fueron: plantas nucleares, prestadores de energía eléctrica, oleoducto y distribuidora de combustible, y de manera indirecta, a prestadoras de salud, confirmando que son blancos

predilectos por los ciberdelincuentes debido a su importancia estratégica y el impacto que genera a la estabilidad organizacional o estatal.

Por su parte, los ataques a Irán y Ucrania fueron con motivos políticos, a diferencia de los ataques realizados en Estados Unidos y Colombia que la motivación fue criminal; sin embargo, sin importar cuál sea la razón del ataque se puede determinar que se menoscaban, afectan o violan derechos humanos de manera directa o indirecta. Por ejemplo, con el ciberataque realizado a Keralty indirectamente se afectó a prestadores de salud, por ello, se puede determinar que la vida se entrelaza y pone en peligro en medio de estas dinámicas de dominación en escenarios que no son necesariamente físicos ni que afectan sólo a la víctima, también a terceros.

4. Derechos Humanos vulnerados en los ciberataques y extensión del DIH

Los derechos humanos son derechos congénitos, inherentes al ser humano. Son interrelacionados, inalienables e interdependientes; y sin distinción por razón de sexo, nacionalidad, etnia o lengua, son universales. En ese sentido, en cualquier órbita en la cual la persona traslade su vida, los derechos humanos se trasladan con él.

Teniendo como principio rector de los derechos humanos la dignidad humana, es imperativo indicar que en el Preámbulo de la Declaración Universal de los Derechos Humanos se considera la dignidad la “base” de la libertad, la justicia y la paz en el mundo, que con su reconocimiento puede lograrse un orden mundial presidio por esta triada de valores superiores que sólo pueden alcanzarse a partir de que la dignidad humana sea salvaguardada (Sánchez Patrón, 2020).

Con los avances tecnológicos también se impacta el ejercicio y goce de derechos, al trasladar la vida el ciberespacio, es posible afirmar que pueden generarse transgresiones en dicha órbita, así mismo y teniendo en cuenta que los derechos consagrados en normativas internacionales como la Declaración Universal de los Derechos Humanos (DUDH) pueden ser gravemente violados a través de ciberataques, afectando múltiples aspectos fundamentales de la vida humana. Además, el debate en torno a la ciberseguridad y los derechos humanos ha sido prominente en foros internacionales. En una reunión del Consejo de Seguridad de la ONU, varios países destacaron la importancia de mantener un ciberespacio abierto, libre y estable donde se respeten los derechos humanos y las libertades fundamentales (Human Rights Watch, 2021).

Se permite a continuación, detallar las principales formas en que estos actos cibernéticos pueden transgredir los derechos humanos como:

4.1. Derecho a la Privacidad

Teniendo en cuenta que la Declaración Universal de los Derechos Humanos establece que nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, garantizando así el derecho a la privacidad (Naciones Unidas, 1948, art. 12). Y en vista de que los ciberataques a menudo se dirigen a la obtención no autorizada de datos personales y sensibles, estos ataques pueden incluir la violación de correos electrónicos, archivos médicos, datos financieros y otra información confidencial, la violación del derecho a la privacidad puede llevar a la exposición pública de información privada, usurpación de identidad, fraude financiero, y chantaje; ademas, las víctimas pueden enfrentar serias consecuencias personales y profesionales, y su confianza en los sistemas digitales puede verse gravemente afectada.

Respeto al derecho a la privacidad que se entrelaza con la intimidad, según la Observación general Nº 16 del Comité de Derechos Humanos de la ONU *"La recopilación y el registro de información personal en computadoras, bancos de datos y otros dispositivos, tanto por las autoridades públicas como por las particulares o entidades privadas, deben estar reglamentados por la ley"* (Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos, 1988, p. 2). En ese sentido, al momento en que se vulnere la privacidad e intimidad por algún ataque en el ciberespacio deben existir consecuencias jurídicas para quien realice los ciberataques y normativa encaminada a la protección de derechos de las víctimas.

4.2. Derecho a la Libertad de Expresión

El derecho a la libertad de opinión y expresión, incluido el derecho de buscar, recibir y difundir informaciones e ideas de toda índole, está protegido por la Declaración Universal de los Derechos Humanos (Naciones Unidas, 1948, art. 19). Así mismo, los gobiernos deben reglamentar y prohibir aquellos discursos que promuevan el odio e inciten a la violencia, pero sin abusar de su autoridad. Amnistía Internacional reitera que:

> el derecho internacional protege la libertad de expresión, aunque hay casos en los que, de conformidad con ese mismo derecho, es legítimo limitarla cuando viola los derechos de otras personas o promueve el odio e incita a la discriminación y la violencia. (Amnistía Internacional, s.f.)

Sin embargo, en vista de que los ataques cibernéticos pueden ser utilizados para silenciar voces disidentes y censurar contenidos, los gobiernos y actores malintencionados pueden usar ataques de denegación de servicio (DDoS) para derribar sitios web de medios de comunicación, redes sociales y blogs. Esto puede limitar la capacidad de los individuos para expresar libremente sus opiniones, acceder a información y comunicarse, y en contextos autoritarios, esta forma de censura cibernética puede ser una herramienta para reprimir la oposición y controlar la narrativa pública.

4.3. Derecho a la Seguridad

El precepto de seguridad como derecho humano desde lo internacional parte desde la Carta de las Naciones Unidas, la cual crea uno de los seis órganos principales de la organización, conocido como el Consejo de Seguridad, el cual tiene como responsabilidad principal mantener la paz y seguridad internacional. Frente al concepto de seguro, conforme lo dispone el Diccionario de la Real Academia Española, es todo lo *"Libre y exento de todo peligro, daño o riesgo"* (Real Academia Española, n.d.). Por lo tanto, resulta necesario determinarlo como uno de los derechos inseparables de la dignidad humana (Chavira Rivera & Rico Espinoza, 2022).

El ser humano tiene la necesidad de buscar seguridad, en el sentido que al momento que se transgrede la seguridad se vulneran los derechos a la salud y vida. En ese contexto, "*la seguridad es un derecho humano, condición necesaria para el funcionamiento de la sociedad y uno de los principales criterios para asegurar la calidad de vida"*. (Cartagena, s.f, p 4)

Conforme a la Declaración Universal de los Derechos Humanos, toda persona tiene derecho a un nivel de vida adecuado que asegure su salud y bienestar, así como los de su familia (Naciones Unidas, 1948, art. 25). Teniendo en cuenta lo anterior, los ciberataques pueden comprometer la seguridad física de las personas al atacar infraestructuras críticas como redes eléctricas, sistemas de transporte, hospitales y sistemas de suministro de agua, la interrupción de

estos servicios esenciales puede poner en riesgo la vida de las personas, causar caos social y económico, y crear un ambiente de miedo e inseguridad.

4.4. Derecho a la Salud

Numerosos instrumentos de derecho internacional reconocen el derecho a la salud como derecho humano, es fundamental e indispensable para el ejercicio y goce de los demás derechos humanos que se enuncian en la Carta Internacional de Derechos, como son la dignidad humana, vida, alimentación, trabajo, educación, libertad, igualdad entre otros. (Comité de Derechos Económicos, Sociales y Culturales [CESCR], 2000). Respecto a las libertades, desde el derecho a la salud también las incluye el no ser sometido a torturas o tratos inhumanos como tampoco ser sometido a tratamiento médico sin el propio consentimiento (Organización Mundial de la Salud, n.d.).

Así mismo, el Comité de Derechos Económicos, Sociales y Culturales del Consejo Económico y Social de las Naciones Unidas (2000), frente el derecho a la salud ha indicado:

> El derecho a la salud no debe entenderse como un derecho a estar sano. El derecho a la salud entraña libertades y derechos. Entre las libertades figura el derecho a controlar su salud y su cuerpo, con inclusión de la libertad sexual y genésica, y el derecho a no padecer injerencias, como el derecho a no ser sometido a torturas ni a tratamientos y experimentos médicos no consensuales. En cambio, entre los derechos figura el relativo a un sistema de protección de la salud que brinde a las personas oportunidades iguales para disfrutar del más alto nivel posible de salud. (p. 3)

Conforme a ello, se puede determinar que los ataques dirigidos a sistemas de salud, incluyendo hospitales y clínicas, pueden comprometer la integridad y disponibilidad de registros médicos y sistemas de gestión hospitalaria, lo que puede llevar a la pérdida de información crítica sobre pacientes, retrasos en los tratamientos médicos, y una atención de salud inadecuada; la interrupción de los servicios de salud puede tener efectos devastadores en la vida y el bienestar de las personas.

4.5. Derecho a la Educación

El derecho a la educación es quizás el más importante de los derechos sociales y uno de los más importantes derechos de los niños, niñas y adolescentes, dado que con a través de la educación el ser humano adquiere las capacidades y condiciones necesarias para vivir en sociedad (UNICEF Colombia, n.d.). Con ello, permite a la persona instruirse con ese objetivo de adquirir conocimientos, en ese sentido, la Declaración Universal de Derechos Humanos (DUDH) en en el numeral segundo del artículo 26 ha dispuesto:

> 2. La educación tendrá por objeto el pleno desarrollo de la personalidad humana y el fortalecimiento del respeto a los derechos humanos y a las libertades fundamentales; favorecerá la comprensión, la tolerancia y la amistad entre todas las naciones y todos los grupos étnicos o religiosos, y promoverá el desarrollo de las actividades de las Naciones Unidas para el mantenimiento de la paz. (Declaración Universal de Derechos Humanos, 1948, art. 26, numeral 2)

En ese sentido, al momento que un ciberdelincuente orienta el ataque cibernético a instituciones educativas puede afectar la disponibilidad de recursos educativos en línea, plataformas de aprendizaje y bases de datos académicas, la interrupción de estos servicios puede impedir que los estudiantes accedan a la educación, afectando su aprendizaje y desarrollo y de acuerdo con Wolff y Lehr (2017), "*las instituciones educativas son objetivos cada vez más frecuentes de ciberataques, lo que pone en riesgo tanto la privacidad de los estudiantes como la continuidad de la educación*" (p. 101); por otro lado, en el contexto de la educación remota, la vulnerabilidad de los sistemas digitales puede tener un impacto aún mayor, como lo manifiesta Amoroso (2012), "*los ciberataques contra instituciones educativas pueden comprometer no solo la seguridad de la información, sino también el acceso equitativo a la educación*" (p. 145).

4.6. Derecho a la Información

El derecho a la información se encuentra ligado al derecho a la libertad, sin embargo, se dispone como un derecho humano autónomo dispuesto en diversos ordenamientos internacionales, como son: la Declaración Universal de Derechos Humanos, la Declaración Americana de Derechos y Deberes del Hombre, el Pacto Internacional de Derechos Civiles y

Políticos, y la Convención Americana de Derechos Humanos (Rodríguez Cañada de Palacios, n.d.).

En ese contexto, los ciberataques pueden ser utilizados para desinformar al público, difundir propaganda o manipular la percepción pública mediante la difusión de noticias falsas y la manipulación de datos, esto puede llevar a la confusión, la toma de decisiones mal informadas y la polarización social y de acuerdo con con Hoffman (2015), "*los ataques cibernéticos contra medios de comunicación e infraestructuras de información representan una amenaza directa al derecho a la información*" (p. 183). Por lo que en palabras de Singer y Friedman (2014), "*los ciberataques no solo amenazan la seguridad nacional, sino que también pueden socavar los derechos fundamentales de acceso a la información*" (p. 72).

Es imperativo señalar que los ataques cibernéticos representan serias amenazas a una variedad de derechos humanos humanos, la naturaleza global y transnacional de estos ataques complica aún más la aplicación de la justicia y la protección de los derechos, por lo que se hace imperativo que a nivel internacional se desarrolle y aplique marcos legales y estrategias efectivas para prevenir, mitigar y responder a estos ataques, asegurando que los derechos humanos sean respetados y protegidos en el ámbito digital. Así mismo, Herbert Lin destaca que los conflictos en el ciberespacio presentan desafíos únicos debido a la dificultad de atribuir los ataques cibernéticos a actores específicos por lo que se hace necesario un marco legal claro (Lin, 2011).

En el mismo sentido, Tilman Rodenhäuser, experto del Comité Internacional de la Cruz Roja (CICR), enfatiza que las operaciones cibernéticas militares durante conflictos armados están reguladas por el DIH. Rodenhäuser argumenta que ignorar la aplicación del DIH a los ciberataques crearía una situación absurda donde se prohibirían ataques físicos a hospitales, pero no los cibernéticos, que pueden causar daños igualmente significativos (Rodenhäuser, 2021).

Así las cosas, dada la gravedad de estos impactos, es pertinente considerar la aplicación del Convenio de Ginebra y sus protocolos en el contexto de los ciberataques en órbitas nacionales y transnacionales; los Convenios de Ginebra, establecen normas que podrían ser relevantes en el ciberespacio, por ejemplo, los principios de distinción y proporcionalidad, que requieren que las partes en conflicto distingan entre objetivos militares y civiles y eviten ataques que causen daños excesivos a civiles, pueden ser adaptados para abordar los ciberataques. La aplicación de los principios podría ayudar a regular las acciones en el ciberespacio, imponiendo límites a los tipos de ciberataques permitidos y estableciendo responsabilidades claras para los actores estatales y

particulares. Además, los protocolos adicionales del Convenio de Ginebra, que amplían la protección a víctimas de conflictos armados, podrían ser interpretados para incluir a las víctimas de ciberataques, garantizando así una respuesta humanitaria adecuada y de acuerdo con Lessig (1999), "*las regulaciones en el ciberespacio deben ser reevaluadas continuamente para mantenerse al día con los avances tecnológicos*" (p. 507).

Finalmente, y teniendo en cuentas el Manual de Tallin 2.0, elaborado por Schmitt (2017), "*los principios del derecho internacional son aplicables a las operaciones cibernéticas*" (p. 45), subrayando la importancia de desarrollar marcos legales claros para mitigar los conflictos cibernéticos sin comprometer los derechos fundamentales de los individuos.

En conclusión, los ciberataques representan una amenaza significativa para los derechos humanos y su gravedad justifica la consideración de normas internacionales como el Convenio de Ginebra y sus protocolos, por lo que adaptar los principios al ciberespacio podría proporcionar un marco legal robusto para proteger a las personas de los impactos negativos de los ciberataques y asegurar que se respeten los derechos humanos en la era digital.

Conclusiones

En la actualidad donde los avances tecnológicos afectan todas las órbitas del ser humano y teniendo en cuenta lo expuesto a lo largo de este artículo, es posible determinar que el ciberespacio usado como campo de batalla vulnera de manera directa e indirecta los derechos humanos.

Ahora bien, dado que no existe una normatividad que regule los ataques en ámbitos virtuales, por lo que en el entendido de que los ciberataques representan una amenaza a la materialización de los derechos humanos, se hace necesario que la normatividad del DIH sea extensiva para con ello, salvaguardar en mayor medida al ser humano y sus derechos. Por otra parte, esto no significa que a medida que la era digital sea parte más esencial de la persona, el derecho no deba ir avanzando con él.

Adicional a ello, en respuesta al temor causado por los ciberataques y a las motivaciones, se requiere el fortalecimiento en medidas de ciberseguridad con un enfoque que garantice la plena protección de derechos humanos, no es posible determinar que el ciberespacio como un escenario

donde se pueda llevar a cabo toda actividad imaginable, incluso con resultados beligerantes o criminales.

Finalmente, entendiendo que es esencial la protección y promoción de los derechos humanos, se deben asegurar las medidas progresivas para que ningún avance tecnológico transgrede o afecte dichos derechos.

Referencias bibliográficas

Amnesty International. (s.f.). Libertad de expresión. Amnesty International. https://www.amnesty.org/es/what-we-do/freedom-of-expression/

Amoroso, E. G. (2012). Cyber Attacks: Protecting National Infrastructure. Butterworth-Heinemann.

Ayala Amaya, J. A. (2020). Los ciberconflictos a la luz del derecho internacional humanitario. Anuario de Derecho Internacional Humanitario, 1(1). https://www.unisabana.edu.co/programas/unidades-academicas/facultad-de-derecho-y-ciencias-politicas/anuariodih/articulos/los-ciberconflictos-a-la-luz-del-dih/

BBC Mundo. (2015, octubre 7). El virus que tomó control de mil máquinas y les ordenó autodestruirse. https://www.bbc.com/mundo/noticias/2015/10/151007_iwonder_finde_tecnologia_virus_stuxnet

BBC Mundo. (2022, marzo 23). ¿Qué es un ciberataque y cómo ha evolucionado? BBC. https://www.bbc.com/mundo/noticias-60850173

Bolívar, L. O. (2018). El derecho a la educación. Corte Interamericana de Derechos Humanos. https://www.corteidh.or.cr/tablas/r25566.pdf

Castells, M. (2001). The Internet Galaxy: Reflections on the Internet, Business, and Society. Oxford University Press.

Chavira Rivera, J. E., & Rico Espinoza, R. M. (s.f.). La seguridad como precepto de derecho humano. Comisión Estatal de Derechos Humanos Jalisco. http://historico.cedhj.org.mx/revista%20DF%20Debate/articulos/revista_No18/ADEBATE-18-art1.pdf

Chipana Luna, R. (2013). Hackers que se pasaron al bando de las empresas. Rebelión Cibernética, 5(1), 41-49. Recuperado de http://revistasbolivianas.umsa.bo/scielo.php?script=sci_arttext&pid=S1997-40442013000100009&lng=en&nrm=iso

Comité de Derechos Económicos, Sociales y Culturales (CESCR). (2000). El derecho al disfrute del más alto nivel posible de salud (Observación General 14) (E/C.12/2000/4). ACNUR. https://www.acnur.org/fileadmin/Documentos/BDL/2001/1451.pdf

Corte Interamericana de Derechos Humanos. (s.f.). Seguridad ciudadana y derechos humanos. https://www.corteidh.or.cr/tablas/r26029.pdf

Crespo-Pazmiño, D. (s.f.). Ciberseguridad y Derechos Humanos: respuestas estatales e individuales a las revelaciones de espionaje de Snowden. (19). 77-98. https://doi.org/10.32719/26312549.2019.19.3

Deibert, R. (2020). Reset: Reclaiming the Internet for Civil Society. House of Anansi Press.

El Confidencial. (2016, enero 21). Amenazas en la oscuridad: cómo los hackers pueden provocar un apagón en tu ciudad. https://www.elconfidencial.com/tecnologia/2016-01-21/amenazas-en-la-oscuridad-como-los-hackers-pueden-provocar-un-apagon-en-tu-ciudad_1138837/

Frederick Rivadeneira, E. (2016). STUXNET, la primera ciberarma. Revista Marina, 2, 76-81. https://revistamarina.cl/revistas/2016/2/efrederickr.pdf

Fondo de las Naciones Unidas para la Infancia (UNICEF). (s.f.). El derecho a la educación. https://www.unicef.org/colombia/media/2241/file/El%20derecho%20a%20la%20educaci%C3%B3n.pdf

García Bordonado, S. (2022). Ciberseguridad: Un estudio sobre las amenazas cibernéticas y las medidas de protección. [Trabajo de Fin de Grado, Universidad Autónoma de Madrid]. Repositorio Institucional UAM. https://repositorio.uam.es/bitstream/handle/10486/698264/garcia_bordonado_sergio_tfg.pdf?sequence=1&isAllowed=y

García Monje, R. A. (2017). Seguridad informática y el malware. [Artículo académico, Universidad Piloto de Colombia]. Repositorio Institucional. https://repository.unipiloto.edu.co/handle/20.500.12277/2641

Hoffman, D. (2015). Cybersecurity and freedom of information: Threats to media freedom and access to information. Journal of Cyber Policy, 1(2), 179-195. https://doi.org/10.1080/23738871.2015.1069820

Human Development Report 1994. (1994). United Nations Development Programme. https://hdr.undp.org/system/files/documents/hdr1994escompletonostats.pdf

Human Rights Watch. (2021). It's time to treat cybersecurity as a human rights issue. Retrieved from https://www.hrw.org/news/2021/07/15/its-time-treat-cybersecurity-human-rights-issue

IBM. (s.f.). Cyber attack. https://www.ibm.com/es-es/topics/cyber-attack

IBM. (s.f.). Cybersecurity. https://www.ibm.com/mx-es/topics/cybersecurity

Infobae. (2024, febrero 20). El avance tecnológico permite que personas con habilidades técnicas limitadas realicen ciberataques de gran impacto. https://www.infobae.com/mexico/2024/02/20/el-avance-tecnologico-permite-que-personas-con-habilidades-tecnicas-limitadas-realicen-ciberataques-de-gran-impacto/

INISEG. (s.f.). Ucrania sufre el primer apagón causado por un ciberataque. https://www.iniseg.es/blog/ciberseguridad/ucrania-sufre-el-primer-apagon-causado-por-un-ciberataque/

Lessig, L. (1999). The Law of the Horse: What Cyberlaw Might Teach. Harvard Law Review, 113(2), 501-549. https://doi.org/10.2307/1342331

Lin, H. (2011). Responding to sub-threshold cyber intrusions: A fertile topic for research and discussion. Georgetown Journal of International Affairs, Special Issue, International Engagement on Cyber: Establishing International Norms and Improved Cybersecurity, 127-135. National Academies Press.

Lutz, B. (2012). La pasión del poder: Teoría y práctica de la dominación. Política y Cultura, (37), 71-90. https://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S0188-77422012000100016

Martínez, R., Palma, A., & Velásquez, A. (s.f.). Revolución tecnológica e inclusión social: Reflexiones sobre desafíos y oportunidades para la política social en América Latina. CEPAL. https://www.cepal.org/sites/default/files/publication/files/45901/S2000401_es.pdf

Microsoft. (s.f.). ¿Qué es el malware? Microsoft. https://www.microsoft.com/es-co/security/business/security-101/what-is-malware#:~:text=El%20malware%20hace%20referencia%20a,dispositivos%20de%20punto%20de%20conexi%C3%B3n%20

Organización de las Naciones Unidas (ONU). (1948). Declaración Universal de Derechos Humanos. https://www.ohchr.org/sites/default/files/UDHR/Documents/UDHR_Translations/spn.pdf

Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos. (1988). Derecho a la intimidad (Art. 17) HRC Observación general Nº 16 (General Comment) 32º período de sesiones. Recuperado de https://www.acnur.org/fileadmin/Documentos/BDL/2005/3584.pdf

Organización Mundial de la Salud. (s.f.). El derecho a la salud. Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos (ACNUDH). https://www.ohchr.org/sites/default/files/Documents/Publications/Factsheet31sp.pdf

Panda Security. (s.f.). ¿Qué es un gusano informático? Panda Security. https://www.pandasecurity.com/es/security-info/worm/

Ramírez Sánchez, J., García López, T., & Bocarando Lara, J. C. (s.f.). Estudio descriptivo del malware en una dependencia académica de una institución pública de educación superior. Universidad Veracruzana. https://www.uv.mx/iiesca/files/2016/11/06CA201601.pdf

Real Academia Española. (s.f.). Diccionario de la lengua española (22.ª ed.). Recuperado de https://www.rae.es/drae2001/seguro

Rockwell Automation. (s.f.). Lecciones del ciberataque a Colonial Pipeline. https://www.rockwellautomation.com/es-co/company/news/articles/lecciones-del-ciberataque-a-colonial-pipeline.html

Rodenhäuser, T. (2021). Cyber Warfare: does International Humanitarian Law apply? International Review of the Red Cross. Recuperado de International Review of the Red Cross.

Rodríguez Cañada de Palacios, E. (s.f.). El derecho a la información como derecho humano: Libertad de expresión y derecho a la información. Orden Jurídico Nacional. http://www.ordenjuridico.gob.mx/Congreso/pdf/79.pdf

Sánchez Patrón, J. M. (2020). La noción de dignidad en la Declaración Universal de los Derechos Humanos. Fiscalía General de Justicia del Estado de México. https://fgjem.edomex.gob.mx/sites/fgjem.edomex.gob.mx/files/files/Acercade/Derechos%20Humanos/2020-Mayo-Junio/LA%20NOCI%C3%93N%20DE%20DIGNIDAD%20EN%20LA%20DECLARACI%C3%93N%20UNIVERSAL%20DE%20LOS%20DERECHOS%20HUMANOS.pdf

Schmitt, M. N. (Ed.). (2017). Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. Cambridge University Press.

Sigholm, J. (2016). Non-state actors in cyberspace operations. Journal of Military Studies 4(1):1-37. Journal of Military Studies 4(1):1-37

Singer, P. W., & Friedman, A. (2014). Cybersecurity and Cyberwar: What Everyone Needs to Know. Oxford University Press.

STUXNET: ¿Qué es y cómo funciona? (s.f.). Avast. https://www.avast.com/es-es/c-stuxnet

STUXNET: La primera ciberarma de la historia. (2022, septiembre 5). Crónica Seguridad. https://cronicaseguridad.com/2022/09/05/stuxnet-primera-ciberarma-historia/

Tabansky, L. (2011). Basic concepts in cyber warfare. Military and Strategic Affairs, 1, 7-131. https://www.inss.org.il/wp-content/uploads/sites/2/systemfiles/(FILE)1308129610.pdf

Universidad Internacional de Valencia. (s.f.). ¿Qué se considera una infraestructura crítica? Recuperado de https://www.universidadviu.com/es/actualidad/nuestros-expertos/que-se-considera-una-infraestructura-critica

Universidad Tecnológica de Pereira (UTP). (s.f.). La historia de los virus informáticos. https://cidt.utp.edu.co/noticias-y-eventos/la-historia-de-los-virus-informaticos/#:~:text=El%20gusano%20Morris%20fue%20uno,el%20Instituto%20Tecnol%C3%B3gico%20de%20Massachusetts

Wolff, J., & Lehr, W. (2017). The Interplay of Cybersecurity, Privacy and Data Protection and the Implications for Data-Driven Innovation. Journal of Cyber Policy, 2(1), 100-118. https://doi.org/10.1080/23738871.2017.1298641