FACULTAD DE DERECHO

LA CIBERGUERRA Y LA APLICACIÓN DE LOS PRINCIPIOS DEL DERECHO INTERNACIONAL HUMANITARIO

PRESENTADA POR

MARYAM SUAREZ VIVES

TESIS PARA OPTAR EL TÍTULO PROFESIONAL DE ABOGADO

LIMA – PERÚ

2015

FACULTAD DE DERECHO

“LA CIBERGUERRA Y LA APLICACIÓN DE LOS PRINCIPIOS DEL DERECHO INTERNACIONAL HUMANITARIO”

Tesis para optar el Título Profesional de Abogado

AUTOR

MARYAM SUAREZ VIVES

Bachiller en Derecho

LIMA, PERÚ

2015

DEDICATORIA

A mis padres, hermana y abuela que fueron el principal motivo para que lograra concluir mi investigación.

Resumen

La guerra cibernética o ciberguerra es un tema nuevo para la Comunidad Internacional y se refiere a los medios y métodos bélicos que consisten en operaciones cibernéticas que alcanzan el nivel de un conflicto armado sea de carácter internacional o no internacional.

El problema principal de esta tesis es ¿En qué medida la creación de un Departamento Especializado en ciberguerra dentro del Ministerio de Defensa del Perú podría garantizar los principios del Derecho Internacional Humanitario?

El objeto materia de análisis son los ataques cibernéticos dentro de los conflictos armados. En ese sentido la hipótesis principal estima que la creación del Departamento Especializado en Ciberguerra garantizaría los principios del Derecho Internacional Humanitario ya que se encargaría de prevenir, planear, coordinar, ejecutar y conducir operaciones cibernéticas defendiendo las redes de información en la ciberguerra.

Para comprobar la hipótesis en el Primer Capítulo se establece los problemas, objetivos y las hipótesis que serán resueltas al concluir la investigación; posteriormente en los demás capítulos se desarrollarán temas como la soberanía internacional en la ciberguerra, la responsabilidad internacional dentro de la ciberguerra, los principios del Derecho Internacional Humanitario, la diferencia entre ataques cibernéticos y la ciberguerra, entre otros. Todo ello nos permitirá elaborar conclusiones y recomendaciones pertinentes.

Introducción

El derecho es una disciplina en constante evolución que necesita estar a la par con el avance del hombre. En ocasiones tenemos desafíos que se nos presentan para poder establecer la solución más idónea; sin embargo los actores que muchas veces realizan esas soluciones no cuentan con los conocimientos adecuados; es por ello que la comunidad jurídica debe proponer y desarrollar investigaciones, no solo para el ámbito interno, sino para el ámbito internacional.

El derecho internacional es una de las ramas más amplias y complejas de esta ciencia. No solo involucra el estudio de nuestro Estado, sino también el de toda la Comunidad Internacional; ello enriquece a nuestras instituciones y a los actores jurídicos.

Una rama del Derecho Internacional es el Derecho Internacional Humanitario, esta disciplina jurídica protege a las personas (combatientes o civiles) en caso de conflictos armados y es un derecho humanista. El DIH ha regulado ciertas armas y/o métodos bélicos con la finalidad de que los conflictos armados sean menos sangrientos, evitando así los daños colaterales y los sufrimientos innecesarios.

A mitad del siglo XX la Comunidad Internacional ya mencionaba algunas armas y métodos que han sido creadas gracias a la evolución del ser humano; estas armas y métodos han resultado en diversas ocasiones un desafío para el Derecho Internacional Humanitario y una preocupación para toda la Comunidad Internacional.

El ciberespacio actualmente es un escenario nuevo de confrontación y requiere, probablemente, de una regulación especial; ello no quiere decir que el Derecho

Internacional Humanitario no se acomode a estos nuevos desafíos. Los Convenios de Ginebra de 1949 y los Protocolos Adicionales de 1977 son normas internacionales que deja abierta la posibilidad de análisis ante estas nuevas armas y/o métodos de los conflictos armados, pero es necesario una regulación especial con la participación de todos los Estado.

En la presente investigación se desarrollará temas de Derecho Internacional Humanitario a la luz de la ciberguerra, se analizará si los ciberataques dentro de un conflicto armado amenaza o no los principios del DIH, se sustentará la necesidad que tiene el Estado Peruano para crear un “Plan estratégico de ciberseguridad” y el “Comité Especializado en Ciberguerra.”

CAPITULO I

Planteamiento del problema

1.1 Descripción de la Realidad Problemática

Los conflictos armados nacen desde que los seres humanos tienen diferentes intereses dentro de una misma sociedad, los pueblos se enfrentan y luchan por lograr una mejora económica, jurídica, política y/o social. Como lo explicó Dunant, H (1982) en su obra cumbre Recuerdo de Solferino; en tiempos normales, el hombre, que generalmente vive en una sociedad organizada lo protegen las leyes; pero en caso de conflicto armado la sociedad se desorganiza perturbándose el medio ambiente natural corriendo peligro la seguridad, salud e incluso la vida de ellos. Es ahí donde nace el Derecho Internacional Humanitario para proteger a las víctimas del conflicto armado y regular los actos hostiles que se desencadenan.

Antes de la regulación del Derecho Internacional Humanitario (DIH) en el sistema internacional actual (Carta de las Naciones Unidas 1945, Convenios de Ginebra de 1949 y los Protocolos Adicionales de 1977); existieron guerras que dieron origen a esta regulación como por ejemplo, la Batalla de Solferino en 1859 la cual tiene como personaje principal a Henry Dunant, considerado padre del Derecho Internacional Humanitario Contemporáneo. Con dicha Batalla el interés humanitario en el marco de un conflicto armado empieza a tener significado, ya que existían armas que producían sufrimientos innecesarios para los combatientes y la población civil.

En épocas remotas los conflictos armados eran reglados por el Derecho Consuetudinario, hoy en día el DIH ha tomado fuerza en la regulación de métodos y prohibición de ciertas armas protegiendo así a la población civil, prisioneros de guerra, heridos y victimas que no se encuentran dentro del conflicto armado. Estos instrumentos conjuntamente con la creación del Comité Internacional de Socorro a los Militares Heridos, poco después Comité Internacional de la Cruz Roja, tienen una preocupación humanista sobre personas en situación de abandono y extremo sufrimiento en que se encuentran los heridos al término de un conflicto armado.

Ahora bien, por otro lado las operaciones militares eran territoriales, marítimas y/o aéreas y tuvieron como medios y métodos de combate diferentes tipos de armas, desde las balas expansivas hasta las bombas atómicas, las cuales fueron un problema de limitación para la comunidad internacional y actualmente se encuentran reguladas conforme a los principios del DIH. Hoy en día, el Derecho Internacional Humanitario enfrenta un desafío de espacio y armas que surgen

con el desarrollo de la tecnología, la cual se ubica dentro de la denominada quinta generación de guerra utilizándose para fines bélicos la informática.

Los Estados como parte de la comunidad internacional necesitan responder a las necesidades de la población civil ya que la nueva tecnología ha ingresado al campo de batalla actual, el ciberespacio, los sistemas de control de armas a distancia, como las aeronaves no tripuladas, los sistemas autónomos, como los robots de combate, serían parte de un nuevo escenario el cual generaría daños y sufrimientos innecesarios a la población civil. No cabe duda, que para estos nuevos retos es necesaria la presencia del DIH en un nuevo campo de batalla, ya que la tecnología puede ser utilizada como un arma evolutiva y sobre todo es necesario saber si este derecho se encuentra o no acorde a dicha evolución.

Las grandes potencias se encuentran más preocupadas que los países subdesarrollados, ya que son quienes han sufrido varios ataques cibernéticos a través de sus ordenadores; recordemos que en el apogeo de la Guerra Fría en junio de 1982 un satélite de EE.UU de alerta temprana detectó una gran explosión en Siberia sobre un oleoducto de gas, una explosión nuclear jamás vista en el espacio, la que se debió a un fallo en el sistema de control que espías soviéticos habían robado a una empresa en Canadá, pero lo que no sabían era que la Central Intelligence Agency (CIA) había manipulado el software para obtener mayor resultado.

En el 2009 el Secretario de Defensa de Estados Unidos, Robert Gates, mediante declaraciones a los medios de comunicación reconoció el ciberespacio como un nuevo escenario de los conflictos armados; de igual manera afirma que la infraestructura digital de Estados Unidos es un activo estratégico nacional. En junio del mismo año creó el llamado “comando cibernético” o “cybercomando”

(USCC), dicha arma es formidable, necesita un mínimo de equipo tecnológico, con el se puede obtener ventajas militares pero su uso indebido puede causar pérdidas de vidas sin distinción entre combatientes y población civil.

Actualmente los trenes, aviones, instalaciones energéticas funcionan a través de aparatos informáticos los cuales son muy propensos de recibir estos ataques. A mediados del 2010, según los medios de comunicación como New York Times, el gobierno de Estados Unidos e Israel financiaron la creación del virus STUXNET, el cual fue lanzado con la finalidad de atacar las centrales nucleares de Irán. Este virus se expandió por gran parte de las redes generando grandes perjuicios para toda la sociedad; se dice que si este virus hubiese llegado a una central nuclear podría haber generado un desastre comparado con el de Chernòvil.

Con lo antes descrito podemos visualizar que estos ataques cibernéticos tanto en tiempo de paz y en tiempo de guerra afectan la paz y seguridad internacional, no cumpliéndose el artículo 2 párrafo 4 de la Carta de Naciones Unidas el cual prescribe: “Para la realización de los Propósitos consignados en el Artículo 1, la Organización y sus Miembros procederán de acuerdo con los siguientes Principios: … 4. Los Miembros de la Organización, en sus relaciones internacionales, se abstendrán de recurrir a la amenaza o al uso de la fuerza contra la integridad territorial o la independencia política de cualquier Estado, o en cualquier otra forma incompatible con los Propósitos de las Naciones Unidas.”

El primer estudio de este nuevo escenario de guerra fue auspiciado por la Organización del Tratado del Atlántico Norte, denominado “The Tallinn Manual on the International Law Applicable to Cyber Warfare” publicado en 2013. Los miembros de la Organización de las Naciones Unidas ya se encuentran

trabajando una propuesta con los Estados para la creación de un convenio que prohíba la guerra cibernética; es preciso mencionar que el Estado Peruano actualmente no cuenta con una política de defensa cibernética, lo cual es preocupante ya que es posible que hoy a través de las redes nos encontremos ante la primera guerra cibernética mundial.

1.2 Formulación del Problema

1.2.1 Problema General

¿En qué medida la creación de un Departamento Especializado en Ciberguerra dentro del Ministerio de Defensa del Perú podría garantizar los principios del Derecho Internacional Humanitario en un ciberguerra?

1.2.2 Problemas Específicos

- ✓ ¿En qué medida el control de los ataques informáticos en una ciberguerra podría garantizar los principios del Derecho Internacional Humanitario?
- ✓ ¿En qué medida el control del ciberespacio por el Departamento Especializado en Ciberguerra podría garantizar los principios del Derecho Internacional Humanitario?
- ✓ ¿En qué medida la prevención de los ciberataques a la población civil podría garantizar los principios del Derecho Internacional Humanitario?

1.3 Objetivos

1.3.1 Objetivo General

Determinar como la creación del Departamento Especializado en Ciberguerra dentro del Ministerio de Defensa del Perú podría garantizar los principios del Derecho Internacional Humanitario.

1.3.2 Objetivos Específicos

- ✓ Determinar como el control de los ataques informáticos en una ciberguerra podrían garantizar los principios del Derecho Internacional Humanitario.
- ✓ Determinar como el control del ciberespacio por la Departamento Especializado en Ciberguerra podría garantizar los principios del Derecho Internacional Humanitario.
- ✓ Determinar como el Departamento Especializado en Ciberguerra puede garantizar a la población civil la aplicación de los principios del Derecho Internacional Humanitario.

1.4 Justificación de la investigación

La investigación a desarrollarse se justifica en primer lugar, desde el punto de vista académico, dado que la ciberguerra es poco estudiada por los especialistas en DIH ya que han desarrollado su estudio en las llamadas, guerras terrestres, aéreas o navales. Con el transcurrir del tiempo los países potencias han desarrollado diversos métodos de ataques a través de las redes de comunicación, siendo importante investigar si dichos ataques se encuentran aceptados y/o prevenidos en el Derecho Internacional Humanitario.

En segundo lugar, es importante que la sociedad conozca sobre el avance de la tecnología y cuanto afecta, este avance, a los sistemas informáticos de cada Estado; ello nos llevará a que se tomen medidas necesarias para capacitar los militares y evaluar la política que tomará cada Estado para prevenir y/o enfrentar la ciberguerra.

Por último, la investigación es transcendente ya que la comunidad jurídica internacional contará con más fundamentos jurídicos necesarios para enfrentar una ciberguerra.

1.5 Formulación de hipótesis

1.5.1 Hipótesis General

La creación del Departamento Especializado en Ciberguerra garantizaría los principios del Derecho Internacional Humanitario ya que se encargaría de prevenir, planear, coordinar, ejecutar y conducir operaciones cibernéticas defendiendo las redes de información en la ciberguerra.

1.5.2 Hipótesis Específicas

H_1. El control de los ataques informáticos en la ciberguerra limitaría los efectos colaterales a la población civil.

H_2. El control del ciberespacio garantizaría el principio de proporcionalidad del Derecho Internacional Humanitario.

H_3. La prevención de los ciberataques a la población civil garantizaría el principio de distinción y limitación del Derecho Internacional Humanitario.

CAPITULO II

La evolución del Derecho Internacional de los Conflictos Armados afronta nuevos retos contemporáneos

Desde los inicios de la historia el hombre ha sufrido enfrentamientos con diferentes medios de ataque; desde el arma más simple o menos dañinas hasta la más compleja.

Estas nuevas armas y/o métodos los conocemos hoy como “los desafíos contemporáneos del Derecho Internacional Humanitario”. Es por ello que en el presente capitulo definiré brevemente el Derecho Internacional Humanitario (DIH para menciones posteriores) o Derecho Internacional de los Conflictos Armados (DICA), el nacimiento y la evolución su codificación la cual será dividida por cuatro subcapítulos.

El primer subcapítulo desarrollará la definición y ámbito de aplicación del DIH o DICA. El segundo subcapítulo se estudiará y analizará el inicio del DICA mediante la costumbre de los Estados, teniendo como fin el Primer Convenio de

Ginebra de 1864. El tercer subcapítulo abarca desde el Primer Convenio de Ginebra (1864) con las posteriores modificaciones realizadas a la normativa que regula el DICA. Por último, el cuarto subcapítulo mencionaré los nuevos retos que se presentan actualmente para la normativa del DICA, teniendo como reto principal, la ciberguerra.

2.1 Definición y ámbito del Derecho Internacional Humanitario o Derecho Internacional de los Conflictos Armados.

Antes de iniciar con la definición de Derecho Internacional Humanitario, es necesario ingresar, en primer lugar, al Derecho Internacional. “El derecho internacional es el conjunto de normas jurídicas que rigen las relaciones de los Estados entre si y también la de éstos con ciertas entidades que, sin ser Estados, poseen personalidad jurídica internacional.” (Ruda, J.M., 1979, pp. 3)

El Derecho Internacional se divide en dos ramas, el Derecho Internacional Público y el Derecho Internacional Privado. El Derecho Internacional Público, es la rama que estudia las relaciones entre Estados y entre estos y los demás sujetos de derecho internacional, así como la organización y funcionamiento de la comunidad internacional. (Monroy M., 2011, p. 3) Muchas veces el Derecho Internacional Público es llamado Derecho Internacional ya que siempre han tenido concepciones similares, pero no vienen hacer lo mismo; el Derecho Internacional Público es parte del Derecho Internacional y se encuentran en relación de parte-todo.

De igual manera manifiesta Monroy M. (2011) “El Derecho Internacional Privado es la rama del derecho público externo que tiene por objeto resolver los conflictos que se presentan cuando en una relación jurídica interviene un elemento

extranjero. Las diferencias entre estas dos ramas del derecho internacional son las siguientes: a) por los sujetos, pues ya hemos visto que el derecho internacional regula relaciones entre Estados, pero hay otros sujetos, como los organismos internacionales, la Santa Sede o Iglesia católica, los rebeldes cuando han sido reconocidos como beligerantes, la Orden Soberna de Malta y el individuo en ciertos casos. En cambio los sujetos del derecho internacional privado son personas naturales o jurídicas de distintos Estados; b) la fuente principal del derecho internacional está constituida hoy por los tratados públicos y en, cambio en el derecho internacional privado, por la doctrina de los autores, puesto que la codificación es todavía muy deficientes y c) por la sanción." (p.6)

Al haber diferenciado el Derecho Internacional Público y Privado, pasaré a definir el Derecho Internacional Humanitario. El Derecho Internacional Humanitario o llamado también Derecho Internacional de los Conflictos Armados es un rama del Derecho Internacional Público; como bien define Arbeláez J. (1975) es "el conjunto de normas jurídicas internacionales, escritas o consuetudinarias, que prescriben la moderación de los conflictos armados entre los pueblos, garantizan el respeto a la persona humana y aseguran el desarrollo completo de la individualidad" (p. 7)

Como también señala Swinarski CH.(1984) "El derecho internacional humanitario es el cuerpo de normas internacionales, de origen convencional o consuetudinario, específicamente destinado a ser aplicable en los conflictos armados, internacionales o no internacionales y que limita, por razones humanitarias el derecho de las Partes en conflicto a elegir libremente los métodos y los medios utilizados en la guerra o que protege a las personas y a los bienes afectados o que pueden estar afectados por el conflicto." (p.11)

Al Derecho Internacional Humanitario también se le denomina “Derecho Internacional de los Conflictos Armados” o Ius in bello” ya que es un conjunto de normas internacionales que regulan la normativa se encuentra vigente dentro de cualquier conflicto armado. Salmòn E. (2004) señala que “El Derecho Internacional Humanitario (DIH) o ius in bello no permite ni prohíbe los conflictos armados, tanto internacionales como internos, sino que, frente a su desencadenamiento, se aboca al fin de humanizarlos y limitar sus efectos a lo estrictamente necesario.” (p.23)

Al referirnos al Derecho Internacional Humanitario tenemos que definir “conflicto armado”; para ello cabe señalar que no existe concepto desarrollado para el término “conflicto armado” en ninguna de las cuatro Convenciones de Ginebra de 1949 y en ninguno de sus Protocolos Adicionales de 1977, lo único que se resalta es que existe en el II Protocolo Adicional requisitos de aplicación de dicho tratado; el Tribunal Penal para la Ex Yugoslavia en el caso de Dusko Tadic planteó que existe conflicto armado cuando “Se recurre a la fuerza entre estados o hay una situación de violencia armada prolongada entre autoridades gubernamentales y grupos armados organizados o entre estos grupos dentro de un Estado.”

El termino conflicto armado se divide en dos partes, conflicto armado internacional (CAI) y conflicto armado no internacional (CANI). El conflicto armado internacional (CAI) no se encuentra definido dentro de los cuatro Convenios de Ginebra; sin embargo, el artículo 1 del Protocolo Adicional I establece los tres supuestos del CAI. El CICR (2008) menciona que “Según esta disposición, un conflicto armado internacional (CAI) es aquel en que se enfrentan “Altas Partes Contratantes”, en el sentido de Estado. Un CAI ocurre cuando uno

o más Estados recurren a la fuerza armada contra otro Estados, sin tener en cuenta las razones o la intensidad del enfrentamiento. “(p.1) Hay que diferenciar entre conflicto armado internacional y guerra, pues “En ese sentido, se debe precisar que la noción de conflicto armado internacional no debe ser entendida en forma unívoca, sino como una situación de hecho existente entre dos o más Estados, que excede la noción tradicional de guerra […]” (Novak, F. 2003, p.209)

En el conflicto armado no internacional (CANI) se encuentra regulado por el artículo 3 común a los Convenios de Ginebra de 1949 y el artículo 1 del Protocolo adicional II. Según Salmón E. (2004) “A diferencia del CAI donde se enfrentan estados y eventualmente, pueblos que luchan contra la dominación colonial, racista u ocupación extranjera, en el caso del CANI se enfrentan grupos de un mismo Estado.” (p. 113)

Al haber diferenciado entre CAI y CANI, nos toca señalar el ámbito de aplicación personal del DIH o DICA en sus dos tipos de conflictos. Para los conflictos armados internacionales “Los principales destinatarios formales de las normas del DIH son los Estados” (Hernández J, 2003, p.81); por otro lado señalan que “Los estados no son solo los requisitos actores de un conflicto internacional, sino que además han concurrido con su consentimiento y con su práctica o anuencia a la configuración del régimen aplicable.” (Salmon, E., 2004, p.81)

En el caso del CANI la aplicación personal se basa, para Hernández J. (2003), “las normas convencionales de DIH destinadas a regular los conflictos armados no internacionales están dirigidas, tanto a los Estados Parte en dichos instrumentos, como a los grupos armados organizados – término que alude de manera general a todo grupo de particulares que se constituye como parte en un conflicto armado – al interior de su territorio.” (p. 111)

Respecto al ratione temporis del Derecho Internacional Humanitario, en la sentencia del caso de Tadic, el Tribunal Penal para la Ex Yugoslavia señaló que “el alcance temporal y geográfico de un conflicto armado se extiende más allá del momento y lugar exacto de las hostilidades.” Esto quiere decir, que para el tiempo del conflicto armado, no hay diferencias entre el CAI y el CANI, solo es necesario la existencia de un conflicto armado.

Se ha realizado un breve comentario sobre la definición y desarrollo del Derecho Internacional Humanitario; ahora es necesario pasar a nuestro siguiente subcapítulo en el cual nos describe la evolución del Derecho Internacional Humanitario a través del tiempo.

2.2 Inicio de un derecho consuetudinario: El Derecho Internacional de los Conflictos Armados mediante la costumbre de los Estados.

Antes de que el Derecho Internacional Humanitario o Derecho Internacional de los Conflictos Armados lograra codificarse universalmente, la guerra se caracterizaba por la ausencia de toda regla con excepción de la “la ley más fuerte” que se practicaba entre los Estados y estos limitaban la guerra; como manifiesta Peytrignet, G. (1995) **“**Bien antes de que naciera la etapa moderna del DIH, existían normas, tanto de costumbre como de derecho, que podían tener aplicación en los conflictos armados. Se trataba de acuerdos, generalmente bilaterales, concluidos antes, durante o después de las hostilidades y que buscaban asegurar un tratamiento recíproco a los heridos o a los prisioneros, fijar los términos de una rendición o de una capitulación, decidir una tregua o un cese al fuego, o simplemente llevar a cabo las acciones humanitarias derivadas de la ejecución de un tratado de paz. Sin embargo, estas normas dependían de

negociaciones frecuentemente injustas, y no gozaban de un respeto universal." (p.146)

Un importante aporte fue la declaración de la guerra, según Diallo, Y. (1978) "El comienzo de las hostilidades también obedecía a ciertas normas como la declaración de guerra – a través de su anuncio mediante redobles de tambor, la emisión de sonidos, de cuernos o el disparo de flechas – o la obligación del aviso adversario de la intención y de los motivos del ataque antes de su inicio." (Como se citó en Novak, F. & otros, 2006). Si bien es cierto esta costumbre no era regla general para todas naciones, pero ya existían y no solo estas, también existían la prohibición de no matar al adversario caído, no herir al enemigo desarmado, luchar frente a frente, no matar a los no combatientes, entre otros.

Una cultura que aporto gran parte de reglas fue la hindú aunque los hindúes no dieron denominación especial alguna al derecho humanitario. El derecho antiguo hindú se basaba en concepto sociológico de una castra sacerdotal y estaba influenciado por dogmas teleológicos y teorías filosóficas. Los hindúes basaban normas relativas a las relaciones interestatales en el Dharma como el último recurso de la humanidad. Otros documentos importantes de la cultura hindú fueron las Leyes de Manú, según Novak F. "En él se proclaman también normas dirigidas a sus guerreros muy avanzadas para la época, como el respeto a las leyes y la población del país enemigo(la cual no era considerada como parte del conflicto); el trato indulgente hacia los heridos en combate (incluso enviándolos a sus hogares después de haberlos curado); la prohibición de atacar tanto a estos como a los desarmados, indefensos y fugitivos; la prohibición de utilizar

armas arpadas o envenenadas (conocidas como armas escondidas); la prohibición de declarar una guerra sin cuartel; y la reglamentación de la requisa, la propiedad enemiga y la cautividad.” (p.37)

Los hindúes no fueron los únicos que aportaron en el Derecho Internacional Humanitario, según Salmón E. (2004) “En Babilonia, en tiempos del rey Hamurabi (1728-1686 a. de C.), se garantizaba la protección de los más débiles; los hititas garantizaban el respeto a la población civil del enemigo y, al igual que los sumerios exigían una declaratoria de guerra para el inicio de la misma y un acuerdo de paz para concluirla, así en el año 1269 a. de C. firmaron un acuerdo de paz con los egipcios dando fin a la guerra entre estos pueblos.” (pp. 58 -59)

Una obra clásica para inicios del Derecho Internacional Humanitario y su posterior desarrollo fue “El arte de la guerra”, según Sun Tzu en toda batalla debe existir un mando o líder y este debe de mostrar inteligencia, sinceridad, humanidad, valor y dignidad. Otro aporte importante ha sido mencionar que la captura del enemigo es preferible a su eliminación y que la peor táctica es el ataque a una ciudad; asediarla solo debía ser considerado como por último recurso.

Grecia estuvo influenciada en el Derecho Natural, tenían respeto a los cadáveres y ritos funerarios, neutralizaron sus santuarios y las propiedades de los dioses; la religión estaba muy arraigada a sus costumbres y esto hacia que se comporten de manera humana por ello empieza a nacer lo que es actualmente llamado derechos humanos.

En Roma, con la influencia de los Estoicos y con la influencia del cristianismo surge lo que hoy se le denomina “guerra justa”. Según Peña L. (2001) “Cicerón formula la teoría de la guerra justa de la siguiente manera: la hegemonía romana se debe a su superioridad en justicia y Derecho, a que sus guerras han sido justas y han traído un orden más justo favoreciendo una sociedad universal regida por el ius gentium. La lucha Romana por el Derecho ha sido premiada por los dioses.”

En la Edad Media, se reformuló la teoría greco-romana de la Guerra Justa y según Pictect, J. (1986) “se trataba nada menos, de justificar la guerra y de sus oprobios a los ojos de los creyentes, por un compromiso entre el ideal moral y las necesidades políticas.” Para San Agustín (1945) “El soberano legítimo tiene el poder de establecer y de mantener este orden. Como el fin justifica los medios, los actos de guerra cometidos por la causa del soberano pierden todo carácter de pecado. Esta guerra es declarada justa, Dios la quiere; a partir de este momento, el adversario es el enemigo de Dios y como tal, sólo podría hacer una guerra injusta.”

El Islam, también tuvo influencia notable en la evolución del DICA, sus creyentes se regían por El Corán, la Sunna y el Itijihab, y estos instrumentos se basan en principios tales como la igualdad entre los hombres, la justicia, la consulta popular y la reciprocidad.

La caballería fue una figura que nació en Francia, los caballeros vieron la necesidad de reglamentar las hostilidades y regirse bajo reglas claras en la

batalla; prohibieron el uso de determinadas armas y normó la declaración de guerra.

Entre los siglos XIV y XV, al finalizar la Edad Media, el cañón y fusil transformarían la humanidad y esto generaría mayores daños y víctimas. Es ahí cuando Hugo Grocio en su obra "De iure belli ac pacis" menciona que la guerra justa no significaba la autorización de una guerra ilimitada y que es lícito todo lo que es necesario para alcanzar el fin. Esto daba entender que el ataque se limitaba al fin que tenía cada batalla y no deberían ser atacados personas u objetos que no cumplieran con el fin. Novak, F. (2003) menciona que "Es a partir de este siglo que las Partes en conflicto – específicamente los jefes de los ejércitos adversarios – van a convenir, principalmente, tres diferentes tipos de pactos: los "carteles" que estaban referidos a la reglamentación del intercambio y rescate de los prisioneros de guerra; las "capitulaciones", que eran los documentos por los cuales se normaban las rendiciones de los fuertes y fortalezas; y los "armisticios", que enunciaban las normas referentes al trato de los heridos y enfermos." (p. 50)

En el siglo XVI surge el Estado y por ello la autoridad ya no la ostenta la iglesia; como menciona Pictect, J. (1986) "[...] la formación de los Estados modernos y la decadencia de la autoridad pontificia condujeron a un nuevo concepto del derecho de gentes, que se convierte en el jus inter gentes, en el cual las entidades políticas ocupan el lugar de los individuos como sujetos de derecho." A partir del siglo XVIII ya se empieza hablar de la humanización de la guerra, esta se convirtió en una lucha entre ejércitos profesionales, las personas civiles

ya no participaban en ella. La guerra ya tenía reglas y estas reglas se convertirían en antecedentes del Convenio de Ginebra de 1864. La humanización de la guerra se hizo más fuerte con la influencia de los filósofos y uno de ellos es Rousseau quien dejó como legajo ideas bases para el moderno Derecho de Guerra. Según Rousseau en su obra “El contrato social” publicado en 1762 menciona “La guerra no es una relación de hombre a hombre, sino de Estado a Estado, en que los particulares no son enemigos más que accidentalmente, no como hombres, ni como ciudadanos, sino como soldados.” (p. 14) Esto hace que los combatientes dejen de ser combatientes cuando ya no ostenten armas, en el caso del combatiente enfermo o herido en campo de batalla vuelve a ser ciudadano ya que no pueden retornar al campo de batalla.

Fue con la Revolución Francesa en 1789 que se dio inicio a la lucha de los derechos humanos como derechos naturales e inalienables del hombre, esto permitió determinar algunos límites en la guerra. Esta guerra se llevó a cabo por motivos ideológicos y dejó desbastadores resultados; esta situación no había mejorado mucho a comienzos de la segunda mitad del siglo XIX cuando estalló la guerra de Italia en 1859 en la que se enfrentaron austriacos contra los franco-italianos. Estos ejércitos chocaron en Solferino fue una de las batallas más sangrientas de la historia, como nos relata Dunant H. (1982) “De los muertos, algunos soldados presentan un semblante tranquilo; son los que, alcanzados repentinamente, perecieron en el acto; pero muchos de ellos están contorsionados a causa de las torturas de la agonía, con los miembros rígidos, con el cuerpo cubierto de manchas lívidas, con las uñas de las manos clavadas

en el suelo, con los ojos desmesuradamente abiertas, con el bigote erizado, con un siniestro y convulsivo rictus que deja ver sus dientes apretados.” (p. 11)

Henry Dunant, suizo, hombre de negocios llegó a Solferino y visualizó toda esta batalla, la cual plasmó en su obra “Recuerdo en Solferino”, en ella concluyó en dos grandes premisas; por una parte, la fundación, en todos los países, de “sociedades voluntarias de socorro para prestar, en tiempo de guerra, asistencia a los heridos” y por otra parte, la formulación de un “principio internacional, convencional y sagrado”, base y apoyo para dichas sociedades de socorro.” (Dunant, H., 1982, p. 32)

A raíz de su obra “Recuerdo de Solferino” , se convocó a una comisión de cinco expertos, dentro ellos estaba Henry Dunant, con la finalidad de estudiar las propuestas humanitarias de Dunant. Esta comisión de cinco se les denominó Comité Internacional y Permanente de Socorro a Militares Heridos, hoy conocido con el nombre del Comité Internacional de la Cruz Roja, estos llegaron a “[…] la primera conclusión a la que arribaron fue la necesidad del carácter neutral que deberían tener los servicios sanitarios como de los enfermeros voluntarios, para evitar así ser atacados o tomados prisioneros.” Seis meses después, el Comité decidió convocar a un congreso internacional en Ginebra y aquí se logró adoptar 10 resoluciones que actualmente son la base del movimiento de la Cruz Roja; posteriormente se realizó una reunión diplomática con diversos Estados para adoptar las resoluciones acordadas en 1863. Esta reunión diplomática tuvo como resultado “la Convención para mejorar la suerte que corren los militares heridos de los ejercicios en campaña” y fue firmada en el año 1864.

Actualmente a esta Convención se le conoce como la primera en codificar el DIH o DICA; como vimos anteriormente las antiguas culturas y civilizaciones ya se preocupaban por reglamentar las batallas y evitar sufrimientos innecesarios; por ello, el intento de codificar la costumbre sobre la guerra siempre ha estado latente y estas aun no siendo imperativas lograron difundirse entre otras civilizaciones.

2.3 La evolución del Derecho Internacional de los Conflictos Armados desde el Primer Convenio de Ginebra 1864 hasta su actual normativa.

Antes del Convenio de Ginebra de 1864, existió otro instrumento igual de importante que dio origen a la codificación especifica del Derecho Internacional Humanitario, este instrumento es el Código de Lieber escrito por Francis Lieber; en el contenían reglas tanto sobre la conducción de las hostilidades en un guerra terrestre como sobre el respeto debido a la población civil, la protección de las personas, propiedades privadas y públicas, el respeto a la religión y la moral, a las artes y las ciencias, heridos, prisioneros de guerra, rehenes y francotiradores.

En el año de 1868 el Zar Alejandro II de Rusia convocó a una Comisión Militar Internacional para el uso de ciertos proyectiles, y esta reunión daría como resultado la Declaración de San Petersburgo en la cual prohíbe el uso del proyectil de peso inferior a los 400 gramos, explosivo o que estuviese cargado con material explosivo o inflamable. Posteriormente a esta declaración le sigue la Declaración de Bruselas del año 1874 y está prohibía el uso de ciertas armas o métodos que pudiesen representar daños o muertes inútiles de seres humanos; también se encargó de los espías, prisioneros de guerra, entre otros.

Manual de Oxford o Manual de Leyes de la Guerra Continental hoy sucedido por el Manual de San Remo sobre el Derecho Internacional aplicable a los conflictos armados en el mar, también fue importante para el desarrollo del Derecho Internacional Humanitario. Este Manual introducía la diferencia entre combatientes y no combatientes, establecía reglas de conducta para las personas civiles, los heridos, enfermos y personal sanitario, el tratamiento de los muertos, de los prisioneros de guerra y los bienes eran temas que también resaltaban en este Manual.

Así como Henry Dunant conjuntamente con los Cinco del Comité no fueron los únicos que se preocupaba de buscar y proponer reglas para la codificación de un Derecho de Guerra. El delegado ruso Frederic von Martens ha sido autor de un valioso aporte para el Derecho Internacional y esta fue La Clausula Martens. "La cláusula fue pronunciada por primera vez en el párrafo 3 de la Declaración del 20 de junio de 1899, leída por Von Martens, quien se desempeña como Presidente del XI Encuentro del Segundo Comité de la Segunda Comisión de la Primera Conferencia de la Haya de 1899." (Miyasaki, Sh. p.2)

Ticehurst, R. (1997) menciona que "La cláusula de Martens forma parte del derecho de los conflictos armados desde que apareciera, por primera vez, en el Preámbulo del (II) Convenio de La Haya de 1899 relativo a las leyes y costumbres de la guerra terrestres: Mientras que se forma un Código más completo de las leyes de la guerra, las Altas Partes Contratantes juzgan oportuno declarar que, en los casos no comprendidos en las disposiciones reglamentarias adoptadas por ellas, las poblaciones y los beligerantes permanecen bajo la garantía y el régimen de los principios del Derecho de Gentes preconizados por

los usos establecidos entre las naciones civilizadas, por las leyes de la humanidad y por las exigencias de la conciencia pública.”

Así se empezó a desarrollar el Derecho de los Conflictos Armados o Derecho Internacional Humanitario hasta el desarrollo de la segunda guerra mundial la cual mostró grandes sufrimientos del hombre moderno en tiempos antiguos, a pesar que ya se habían establecido normativa con relación a la guerra. El CICR (Comité Internacional de la Cruz Roja lo que era antes el Comité de los Cinco) convoco a diversas conferencias para el estudio de propuestas. En abril de 1949 se dio nuevamente una conferencia diplomática que tuvo como resultado 4 acuerdos a) I Convenio de Ginebra para aliviar la suerte que corren los heridos y los enfermos de las fuerzas armadas en campaña, que reemplaza los Convenio de 1864, 1906 y 1929. B) II Convenio de Ginebra para aliviar la suerte que corren los heridos, enfermos y náufragos de las fuerzas armadas en el mar, que reemplaza la Convención X de la Haya de 1907, c) III Convenio de Ginebra relativo al trato debido a los prisioneros de guerra, que reemplaza el Convenio de 1929 y d) IV Convenio de Ginebra relativo a la protección debida a las personas civiles en tiempo de guerra, que es un texto innovador, aunque se basaba en las normas pertinentes de la Convención de La Haya y de Ginebra. Posteriormente a mediados de los años 70 el CICR se preocupaba por dos cosas a) proteger a la población civil de la guerra y b) perfeccionar el articulo 3 común; esto dio resultado la aprobación de dos Protocolos Adicionales a los Convenio de Ginebra de 1949, con fecha 8 de junio de 1977: Protocolo I relativo a la protección de las víctimas de los conflictos armados internacionales y el Protocolo II referente a la protección de las víctimas en los conflictos armados no internacionales.

A partir de la aprobación de los instrumentos internacionales antes mencionados, se continuaron estudiando y preparando otros instrumentos que van conforme a los métodos y armas que están apareciendo.

2.4 Los desafíos contemporáneos del Derecho Internacional Humanitario

Como mencionamos líneas arriba, el Derecho Internacional Humanitario está evolucionando ya que existen nuevas armas o métodos de combate; las cuales son creadas por el ser humano conforme su evolución. Estas armas o métodos actualmente se colisionan con el Derecho Internacional Humanitario y en muchas ocasiones, como bien lo menciona el Comité Internacional de la Cruz Roja (2013) pone a debate “la noción y tipología de los conflictos armados, incluida la cuestión de si la clasificación de los conflictos armados que establece el DIH en conflictos armados internacionales y conflictos armados no internacionales es suficiente para abarcar los tipos de conflictos armados que libran en la actualidad.”

Si bien es cierto estas nuevas armas actualmente están reguladas por el artículo 36 del Protocolo adicional I a los Convenios de Ginebra en el cual menciona “Cuando una Alta Parte Contratante estudie, desarrolle, adquiera o adopte una nueva arma, o nuevos medios o métodos de guerra, tendrá la obligación de determinar si su empleo, en ciertas condiciones o en todas las circunstancias, estaría prohibido por el presente Protocolo o por cualquier otra norma de derecho internacional aplicable a esa Alta Parte Contratante”; esto siempre no es así, ya que en la práctica los Estados generalmente esperan llegar a un consenso que determine si un arma es aceptable o no para un comunidad internacional.

Dentro de los nuevos retos que enfrenta el Derecho Internacional Humanitario según el informe emitido por la XXXI Conferencia Internacional de la Cruz Roja y de la Media Luna Roja realizada en Ginebra-Suiza en el año 2011, encontramos la ciberguerra, los sistemas de armas de control remoto, sistemas automatizados de armas y las armadas automatizadas.

Se explicará brevemente cada uno de estos nuevos retos contemporáneos.

- **Ciberguerra**

La ciberguerra es uno de los retos más latentes del Derecho Internacional Humanitario, ya que presenta una serie de figuras que anteriormente no habían sido visualizadas en el DIH, la violación de la soberanía estatal, la regulación del ciberespacio, la vulneración de los principios del DIH y los ataques a la población civil de manera indiscriminada. Si bien es cierto este tema es nuevo para algunas naciones como por ejemplo para Perú; se puede mencionar que ya exiten organismos, incluso personas que se han ocupado de tratar de resolver algunas interrogantes que planteamos sobre la ciberguerra en el Derecho Internacional Humanitario. El Comité Internacional de la Cruz Roja actualmente se encuentra estudiando el presente tema; en una de sus publicaciones el CICR (2013) menciona que “El ciberespacio ha abierto un nuevo escenario de guerra posible. Las partes en conflictos armados recurren cada vez más a sistemas de control de armas a distancia, como las aeronaves no tripuladas. Los sistemas de armas automatizados también se utilizan con mayor frecuencia, y se están estudiando algunos sistemas autónomos, como los robots de combate, para su uso futuro en los campos de batalla.”

No se abordará mucho en el tema ya que es materia de la presente investigación y será desarrollada en los subsiguientes capítulos de manera minuciosa.

- **Sistemas de armas de control remoto**

Se le considera armas de control remoto a aquellas que realizan un ataque remoto, esto quiere decir, que el ataque debe ser iniciado por un operador que se ubica distante al lugar donde se causará la lesión o destrucción; operador que resultará siendo responsable de cualquier lesión y/o violación al Derecho Internacional Humanitario.

Boothby, W. (2012) señala que "[…] el operador debe tener cuidado constante para proteger a los civiles y los bienes de carácter civil cuando se lleva a cabo operaciones militares en general; debe hacer todo lo posible o factible para verificar que los objetivos que se ataquen no sean personas civiles ni bienes de carácter civil y que no están sujetas a protección especial, por lo que son objetivos militares y que no están prohibidos de atacar; debe tomar todas las precauciones posibles o realizar la elección de los medios y métodos de ataque de manera correcta con el fin de evitar, y en todo caso reducir al mínimo, el número de muertos y de heridos entre la población civil, o daños a bienes de carácter civil; él debe abstenerse a decidir un ataque que se puede esperar que sea desproporcionado para los civiles y causen daños incidentales; por ello debe asegurar de que la advertencia previa sea eficaz para que los civiles que puedan ser afectados por el ataque a menos que las circunstancias no lo permitan; por último, debe garantizar que cuando se pueda elegir entre varios objetivos

militares para obtener una ventaja militar equivalente, el objetivo seleccionado debe ser el objetivo correcto.” (pp.588 – 589)

Como bien se ha dicho anteriormente el Comité Internacional de Cruz Roja (2011) señala que “una de las características principales de los sistemas de armas de control remoto es que los combatientes puedan estar físicamente ausentes de la zona de operaciones de combate.” (p. 44); este ataque te permite que se disminuya el número de daños a la población civil pero en otras ocasiones no sabes que daño colateral les puede afectar ya que es impredecible.

La actual doctrina señala que este sistema de armas de control remoto se encuentra en diferentes armas y también se encuentra relacionado de una u otra manera con los ciberataques.

- **Sistemas automatizados**

El CICR (2011) define al arma automatizada de la siguiente manera “Un arma automatizada o un sistema automatizado de armas es aquel que puede funcionar de manera autónoma e independiente aunque para desplegarlo o dirigirlo se requiera la intervención inicial de una persona. Entre los ejemplos de esos sistemas cabe mencionar los cañones centinelas automatizados, municiones con espoleta equipada de sensor y algunas minas terrestres antivehículo.” (p.46) La normativa del DIH corre peligro ya que puede ser vulnerado de diversas maneras; por ejemplo, estos sistemas no tienen la capacidad de distinguir entre un objetivo militar y otro civil, ni mucho menos evaluar si el ataque va a ser o no

proporcional; por lo que su ataque afectaría los principios básicos del Derecho Internacional Humanitario.

- **Sistemas de armas autónomos**

En la XXXI Conferencia Internacional del Movimiento Internacional de la Cruz Roja y de la Media Luna Roja, se define como “Un sistema de armas autónomo es aquel que puede captar o adaptar su funcionamiento según la variación de las circunstancias del entorno en el que es desplegado.” (CICR, 2011, p. 45)

Estas armas son aquellas que actualmente representan un desafío para el Derecho Internacional Humanitario y para la Comunidad Internacional. Con los sistemas de armas autónomos no se puede salvaguardar los principios del DIH; es por ello que surge una serie de interrogantes que aún no han tenido respuestas, como por ejemplo ¿estas armas son licitas o ilícitas? ¿el uso de estas armas está constituido como crimen de guerra?, entre otras.

Se acaba de describir de manera breve cuales son las armas contemporáneas y cuáles son los efectos que tiene de acuerdo con la normativa vigente del Derecho Internacional Humanitario. Como bien se señaló, la presente investigación intenta resolver algunas preguntas planteadas para la ciberguerra; para ello es necesario analizar la ciberguerra en sus diferentes contextos. .

CAPITULO III

La Ciberguerra y la soberanía estatal afrontan un problema en el Principio de No Intervención de los Estados

Uno de los problemas más latentes en la comunidad internacional es determinar si los ciberataques vulneran la soberanía estatal afectando el principio de no intervención de los Estados. En el presente capítulo se abordará de manera breve estos temas ya que es conveniente determinar si los ataques cibernéticos vulnerarían o no la soberanía de un Estado y así poder llegar a nuestro objetivo principal que es la creación de una dirección para operaciones cibernéticas.

3.1 La soberanía de los Estados: Concepto y alcances

La soberanía es el resultado de un proceso histórico. En la antigüedad, la vida social se veía influenciada del cristianismo y es por ello que la iglesia era quien predominaba en el poder; de ahí en adelante el Estado tendría un fuerte antagonista que vino a crear polémicas entre los mismos doctrinarios y las

preguntas que surgían eran ¿Cuál de las dos era superior al otro? Y ¿Quién se debía a quién? Existían dos clases de poderes: Terrenal y Eclesiástico. El poder eclesiástico lo tenía el Papa quien ejercía su poder sobre las autoridades terrenales; sin embargo estas autoridades no fueron capaces de resolver los problemas existentes. Los Papas del Renacimiento renunciaron a la concepción de representar una supremacía y como consecuencia de ello y de las guerras se impuso el modelo del Estado Soberano. El Estado soberano, "el cual es independiente y supremo. Con respecto a la independencia, se mira principalmente a las relaciones internacionales y como consecuencia de ello, el Estado tiene su existencia en el plan de igualdad con respecto a los demás Estados, es decir, no puede estar subordinado a otro Estado, ya que, de lo contrario su soberanía estaría menguada." (Guerrero, J., 1988, p. 501)

La soberanía es un poder del Estado, sin soberanía no existe; entonces quiere decir, que paralelamente es un elemento constitutivo y por tanto es un derecho de todo Estado para que este pueda existir. Según Herdegen, Matthias (2005) "La expresión clásica del derecho de exclusividad vinculado a la soberanía territorial se encuentra en el laudo arbitral de Max Hurber en el caso de la Isla de Palmas (1928):

> La soberanía en las relaciones entre Estados significa independencia. Independencia respecto de una porción del globo es el derecho de ejercer allí, con exclusión de cualquier otro Estado, las funciones de un Estado. El desarrollo de la organización nacional de Estados durante las últimas centurias y, como corolario, el desarrollo del derecho internacional, han establecido este principio de exclusiva competencia del Estado en relación con su propio territorio en forma tal que lo convierte en el punto

de partida para solucionar la mayor parte de los cuestionamientos que conciernen a las relaciones internacionales (RIAA,II, p.829)”

El derecho internacional regula derechos y deberes que corresponden a los Estados como sujetos de Derecho Internacional; existen diversas opiniones de la existencia de ellos, según Accioly H. (1946) “distingue dos categorías en los derechos y deberes, comprendiendo la primera los que los autores han denominado fundamentales, esenciales, innatos o permanentes y la segunda los que son llamados accidentales, secundarios, adquiridos o contingentes. Los primeros son la consecuencia de la propia existencia del Estado o de su condición de miembro de la comunidad internacional. Los segundos derivan de un derecho fundamental o resultan de un tratado o convención internacional o de las costumbres y se refieren a situaciones particulares y variables.”(p. 202) El primer derecho de un estado es el derecho a la existencia y este trae como nexo diversos derechos, encontrándonos con el derecho a la libertad que implica necesariamente los derechos de soberanía interna y externa. .

Diversos autores señalan que la soberanía es un derecho absoluto de los Estados lo cual no es así, pues desde la existencia de la comunidad internacional y sus normas regulatorias para diversas situaciones, esta independencia va a estar limitada por dichas reglas; por lo cual se podría decir que le genera un límite. Como precisaHerdegen, Matthias (2005) “Para los efectos del derecho internacional, la noción de “soberanía” comporta en ella misma la exclusividad, la autonomía y la plenitud de la competencia territorial, pero es obvio que dichos atributos de la “soberanía” no pueden concebirse de manera absoluta, más que cuando se hace referencia al orden jurídico interno, pues en el orden internacional tales atributos se vuelven relativos.” (p.924)

Para el derecho internacional público “los elementos exclusivos y supremos de la soberanía tienen un significado diferente. Mientras que cada Estado posee derechos exclusivos y supremos dentro de su territorio, dicha exclusividad y supremacía encuentran límites frente a la exclusividad y supremacía de otros Estados en sus territorios. En el derecho internacional público, esta limitación inherente es paralela al principio de la no interferencia. Como ya se señaló, en el artículo 2 (7) de la Carta de Naciones Unidas se especifica que otros Estados y las Naciones Unidas no pueden interferir con la soberanía de sus Estados miembros. Los Estados respetan los derechos soberanos, exclusivos y supremos de los otros Estados en sus territorios respectivos. De forma indirecta, la limitación inherente de la exclusividad y supremacía de la soberanía revela igualdad de los Estados.” (Stefan, 2015, p. 88)

Existen tres dimensiones de soberanía: Según Novak, F. (2001) “La soberanía interna, conocida también como autonomía, consiste en el derecho del Estado de escoger libremente su sistema de gobierno, establecer sus leyes y determinar su organización política y administrativa; la soberanía externa, llamada también “independencia”, permite al Esto determinar libremente sus relaciones diplomáticas con otros Estados, decidir su participación en organizaciones y conferencias internacionales, así como sus relaciones económicas internacionales.” (p. 40-41) Para complementar estas dimensiones, tenemos la existencia de una tercera dimensión de soberanía, denominada *soberanía territorial*; “La soberanía territorial, es la autoridad que ostenta el Estado, de manera exclusiva, sobre toda su población y cosas que se encuentren dentro de territorio. (Nkambo, 1999, p. 264 citado en Revilla, 2002).

En resumen la soberanía es la mera autoridad que tiene el Estado para normar, decidir y ejecutarlas las decisiones con sus instituciones, personas y cosas que se encuentran dentro de su territorio sin intervención de ninguna entidad u otro Estado. Esto no quiere decir que el derecho del Estado es absoluto ya que siempre debe respetar los lineamientos del Derecho Internacional. Como bien manifiesta Revilla, Pablo (2002) “Empero, esto no significa que la soberanía tiene carácter absoluto su límite se encuentra en el Derecho Internacional, es decir, si un Estado actúa conforme al Derecho Internacional no viola la soberanía de otro.”

La soberanía externa no es del todo absoluta ya que tiene sus límites establecidos por el Derecho Internacional y se puede ser intervenida en ciertos casos. Existe en el Derecho Internacional el principio de no intervención de los Estados el cual ampara a la soberanía, este principio, como lo veremos a continuación, está amparado en la Carta de Naciones Unidas; pero al igual que toda regla este principio tienes sus excepciones. Por ello se puede decir entonces que “La soberanía implica que un Estado puede controlar el acceso a su territorio y, en general disfruta, dentro de los límites establecidos por tratados y el derecho internacional consuetudinario, el derecho exclusivo de ejercer la jurisdicción y autoridad en su territorio. Las excepciones incluyen el uso de la fuerza en ejercicio del derecho de legítima defensa y de acuerdo con las acciones autorizadas o impuestas por el Consejo de Seguridad de las Naciones Unidas.” (Manual de Tallin)

3.1.1 La soberanía y el ciberespacio

El ciberespacio es un nuevo escenario para que se desarrollen los conflictos armados. La Publicación Conjunta 1-02 del Departamento de Defensa de

Estados Unidos lo define como: “un dominio global dentro del entorno de la información, compuesto por una infraestructura de redes de tecnologías de información interdependientes, que incluye internet, las redes de telecomunicaciones, los sistemas de información y los controladores y procesadores integrados junto con sus usuarios y operadores.” (Gomez, 2012, pp. 170-171)

De otro lado, el “ciberespacio” (también llamado ciberinfinito), es una realidad – espacio virtual, ya que no tiene una locación física espacial… y se encuentra dentro de todas las computadoras y redes de todo el mundo. (Aguirre G. 2007)

A mediados de 2010, el Subsecretario de Defensa de los Estados Unidos William Lynn señaló que el ciberespacio “debe ser reconocido como un territorio de dominio igual que la tierra, el mar y el aire en lo relativo a la guerra.” (PellerinCheryl, 2010 citado en G. Eissa, S., Gastaldi, S., Poczynok, I. y Zacarías, M., 2012).

En este mismo sentido, en la Cumbre de la OTAN en Lisboa de Mayo de 2010, el General norteamericano Keith Alexander indico que el ciberespacio debía “militarizarse” para proteger el derecho a la privacidad de los americanos (Joayanes Aguilar, 2010, citado en G. Eissa, S., Gastaldi, S., Poczynok, I. y Zacarías, M., 2012).

La pregunta que surge con respecto al tema es **¿Los Estados tienen o no soberanía sobre el ciberespacio?** La soberanía la ejerce un Estado sobre su territorio y población (entiéndase por territorio de manera general aire, mar y tierra); **pero ningún Estado puede reclamar soberanía sobre el ciberespacio**. **Lo que sí se puede decir es que todos los Estados tienen soberanía sobre**

sus infraestructuras cibernéticas y son responsables de todas las actividades que realizan dichas infraestructuras.

Según Schmitt, M (2013/2015) **"**La soberanía de un Estado sobre la infraestructura cibernética dentro de su territorio tiene dos consecuencias. En primer lugar, que la infraestructura cibernética está sujeta a control legal y regulatorio por el Estado. En segundo lugar, la soberanía territorial del Estado protege las infraestructuras cibernéticas. No importa si pertenecen al gobierno o a entidades privadas o particulares, ni a los fines que sirve la materia." (p.25) Las infraestructuras cibernéticas de un Estado se pueden localizar dentro del propio Estado o en un lugar distinto del Estado, pero que se encuentran bajo su control; si éstas son atacadas y generan un daño se vulnera la soberanía del Estado a que pertenece dicha infraestructura.

Ya que los Estados no pueden tener soberanía sobre el ciberespacio, estos pueden ejercer su jurisdicción en las actividades ilícitas que ocasionen los ciberataques. Así señala Schmitt, M (2013/2015) ""Sin perjuicio de las obligaciones internacionales aplicables, un Estado puede ejercer su jurisdicción: a) Cuando las personas dedicadas a actividades cibernéticas se encuentren en su territorio; b) Cuando la infraestructura cibernética este situada en su territorio y c) con carácter extraterritorial, de conformidad con el derecho internacional."(p.27)

La jurisdicción en el ámbito territorial "En un sentido más estricto, el vocablo es utilizado frecuentemente para referirse al ámbito territorial dentro del cual la autoridad investida de la potestad jurisdiccional está facultada para realizar funciones." (Ortega, M., 1990, p.128) Para el Derecho Internacional la soberanía abarca el conjunto de competencias estatales que un Estado puede ejercer en

su territorio. Según Dupuy P. (1998) “Las competencias territoriales del Estado toman su carácter de la doble naturaleza del territorio del Estado. Esta es en principio un objeto, es decir un bien sobre el cual el Estado puede ejercer lo que en derecho privado le llamarían derechos reales, a la manera de aquellos que el propietario privado detenta sobre un fundo que le pertenece. Pero el territorio es igual un espacio, habilitado por una población respecto de la cual el gobierno de ese Estado puede ejercer su autoridad. […] La competencia territorial agrupa a ambas, puesto que se debe entender como la aptitud del Estado para ejercer su autoridad conforme al Derecho Internacional tanto sobre las bienes como las situaciones, las personas y las actividades situadas o ejercidas al interior de su territorio.” (p. 59)

Esta jurisdicción no es absoluta, “el Derecho Internacional otorga la inmunidad soberana sobre ciertos objetos que se utilizan para fines gubernamentales no comerciales independientemente de su locación.” (Schmitt, 2013/2015, p. 32) Esta conclusión se llegó en base a la interpretación de la Convención de las Naciones Unidas sobre las inmunidades jurisdiccionales de los Estados y de sus bienes; y como toda regla esta tiene su excepción, según los Convenios de Ginebra todos los objetos que sean considerados objetivos militares pueden ser atacados, quiere decir que se pierde la inmunidad soberana cuando son calificados objetivos militares dentro de un conflicto armado.

3.2 Principio de No Intervención y la Responsabilidad Internacional de un Estado.

El principio de No Intervención se encuentra regulado en el artículo 2 párrafo 7 de la Carta de Naciones Unidas y tiene como fin respetar la soberanía que tiene todo Estado. De igual manera este principio pone una excepción la cual es “la

intervención” como medio de resolver las controversias a través del Consejo de Seguridad.

Para llegar al principio de No Intervención es necesario abordar el tema de la intervención internacional de los Estados. “La intervención, que es la injerencia coactiva de un Estado en las cuestiones externas o internas de otro, constituye una de las más antiguas prácticas de la vida internacional, especialmente en las relaciones de los pueblos fuertes o de las coaliciones de varios Estados, con pueblos débiles o aislados políticamente.”(Ulloa, A., 1957, p. 317)De igual manera Gómez-Robledo, A. (1993) menciona que “[…] el término de “intervenir” tiene diversos alcances, ya que por una parte se habla de un “derecho de intervención”, derecho reivindicado por todos los Estados para proteger a sus ciudadanos y propiedades en el extranjero, y por otra parte se emplea el mismo término para designar la acción imperativa de un Estado que por medio de la amenaza o uso de la fuerza trata de imponer un particular punto de vista sobre un asunto que es de competencia esencialmente doméstica.” (p. 87)

Por regla general tenemos que no está permitido que los Estados intervengan en asuntos internos de otros Estados, pero encontramos excepciones; entre ellas encontramos a) Cuando se plantea el respeto al derecho de conservación o que exista lesión evidente a los intereses de cuya existencia depende la vida colectiva de los Estado, b) Por existencia de un tratado, c) Cuando se realice una contra intervención y d) Intervención por causa humanitaria. Esta última excepción es llamada también injerencia por humanidad la cual según Ulloa, A. (1957) menciona que es “Una razón de humanidad la que determina a intervenir para proteger las vidas de los nacionales del Estado interventor y para impedir las hostilidades y persecuciones religiosas que frecuentemente han degenerado

en ataques sangrientos. El carácter humanitario ha justificado muchas veces que la intervención no solo se prosiga en favor de los nacionales del Estado interventor, sino también de los de cualquier Estado o de los del propio Estado intervenido. En tales casos no se ha tratado de proteger a seres humanos contra quienes las pasiones excitadas determinaban agresiones brutales."(p. 339)

Uno de los antecedentes importantes para este tema es el caso de Actividades Militares y Paramilitares de Estados Unidos contra el gobierno de Nicaragua, la Corte Internacional de Justicia concluyó que "[…] el principio le prohíbe a todos los Estados o grupos de Estados intervenir directa o indirectamente en los asuntos internos o externos de otros Estados. Las intervenciones que se prohíben deben recaer por consiguiente sobre aquellas materias en las cuales a todo Estado le está permitido, por el principio de soberanía, decidir libremente. Dentro de ellas se encuentran el optar por un sistema político, económico, social y cultural, así como la formulación de la política extranjera. La intervención es ilícita cuando utiliza métodos de coerción sobre tales opciones las cuales deben permanecer libres de toda intervención. El elemento de la coerción, que define la intervención prohibida, y que por tanto constituye la esencia de la misma, es particularmente obvio en el caso de una intervención que hace uso de la fuerza, ya sea en forma directa a través de una acción militar o en forma indirecta mediante el apoyo de actividades armadas, terroristas o subversivas, en otro Estados (Case Cocerning Military and Paramilitary Activities in and against Nicaragua (Nicaragua vs. USA), ICJ Reports, 1986, pp. 12 y ss.)

3.2.1 Los ciberataques y el principio de no intervención

Una vez analizado el principio de no intervención es importante determinar de qué manera los ciberataques afectan o no dicho principio. En un primer momento se concluye que toda intervención cibernética es una violación del principio de no intervención o de la soberanía; en el Derecho Internacional al hablar de intervención cibernética podemos referimos a un espionaje o un operación determinada la cual es realizada a través del ciberespacio. Según asegura el abogado y especialista en Derecho Internacional Alba M, (2013) “el espionaje es condenable desde el punto de vista diplomático, puesto que supone una ofensa contra la buena fe que debe prevalecer en las relaciones entre Estados. Sin embargo, desde el punto de vista jurídico, lo cierto es que no existe una norma expresa que prohíba el espionaje entre las naciones.”;

De lo expuesto se deduce que, el espionaje no genera responsabilidad internacional de un Estado y por ello se determinaría que no violaría la soberanía ni el principio de no intervención.

Este argumento se encuentra errado; si hablamos de responsabilidad estatal nos remitimos a la Resolución 56/83 emitida por la Asamblea General de Naciones Unidas en la cual se aprueba artículos sobre responsabilidad del Estado por hechos internacionalmente ilícitos, esta resolución cambia todo nuestro punto de vista. Asimismo, hay que tener en cuenta que existen principios de convivencia y buena vecindad aplicables del derecho internacional.

En el caso del espionaje o cualquier ciberataque muchas veces no genera un impacto en la responsabilidad del Estado y puede ser tratado de manera interna,

por ello no están calificados como elementos coercitivos (amenazas) o usos de la fuerza para ser considerado hechos internacionalmente ilícitos.

Según Schmitt, M. (2013) “Para que un ataque cibernético o el ciberespionaje pueda ser considerado relevante para el Derecho Internacional este debería generar un daño a una infraestructura cibernética de otro Estado; entonces es ahí donde se generaría responsabilidad internacional del Estado.”

En el derecho internacional de los conflictos armados el tema de espionaje se encuentra regulado en el artículo 46 del Protocolo I adicional a los Convenios de Ginebra del 12 de agosto de 1949 relativo a la protección de las víctimas de los conflictos armados internacionales. Antes del Protocolo mencionado el espionaje se regulaba en el Reglamento de la Haya 1907; el artículo 29 determina que el espía es “el individuo que obrando clandestinamente o con falsos pretextos recoja o trate de recoger informes en la zona de operaciones de un beligerante, con la intención de comunicarlos al enemigo.”

Esta definición aún se conserva y se complementa actualmente con el Protocolo I adicional, de ello se desprende que no podrá considerarse como espía al que busque información llevando el uniforme de sus fuerzas armadas.

Segùn Pictet J.& otros, (2001) señalan que “En el IV Convenio, en articulo 5 apartado 1, se establece, en efecto que esas personas, que pueden ser también espías o personas sospechosas de espionaje, no podrán ampararse en los derechos y privilegios conferidos por el Convenio que, de aplicarse en su favor, podrían perjudicar a la seguridad del Estado, aunque no quedan, por supuesto, privarlas de su derecho a un proceso equitativo y legítimo (apartado 3). (p.783)

De igual manera es importante mencionar que en el caso de que existan dos presunciones concurrentes: prisionero de guerra o espía; la de prisionero de guerra deberá primar sobre la de espía al menos mientras que el interesado no esté inculpado por cargos suficientes.

Destacamos entonces, que los ciberataques si violan la soberanía estatal y el principio de no intervención, salvo las excepciones correspondientes (según Carta de Naciones Unidas, legítima defensa e intervención humanitaria) y el ciberespionaje puede ser un ciberataque dentro de un conflicto armado que tendrá relevancia y generará responsabilidad estatal siempre y cuando se dé un daño dentro de una infraestructura cibernética estatal.

CAPITULO IV

¿Ataques informáticos o ciberguerra?

Los ataques informáticos muchas veces son confundidos con la ciberguerra. Las fuentes de información, como periódicos, televisión, emisoras, entre otros, mencionan que actualmente estamos ante la primera ciberguerra. Lo que no tenemos claro es ¿Qué es la ciberguerra? ¿Cómo se desarrolla una ciberguerra? ¿Qué normativa se le aplica a la ciberguerra? ¿La ciberguerra son los ataques informáticos? ¿Cuál es su diferencia? Todas estas preguntas surgen si no sabemos diferenciar los ataques informáticos de una ciberguerra.

Antes de empezar este capítulo señalo que hasta el momento no se ha desarrollado una ciberguerra; lo que sí está sucediendo y que hasta el momento se siguen dando son ataques informáticos que generan un daño grave a la población.

4.1 Ataques informáticos

Actualmente no se ha encontrado ningún ataque informático que dé como resultado una ciberguerra propiamente dicha ya que no se ha registrado dentro de un conflicto armado un ciberataque que dañe de manera concreta una infraestructura Estatal y genere consecuencias graves para el Estado y para la población civil.

El ciberataque se realiza por medio del ciberespacio, y su calificación de ataque armado es depende del contexto en se desarrolle. “Un ciberataque consiste en cualquier acción destinada a socavar las funciones de una red informática para un fin de seguridad política o nacional.” (Hathaway, A. Crootof, R. Levitz, P. Nix H. Nowlan, A. Perdue, & W. Spiege J., 2011, p. 10)

Los ataques por redes informáticas han sido definidos como toda medida hostil contra el enemigo cuya finalidad sea “descubrir, alterar, destruir, interrumpir o transferir datos almacenados, procesados o transmitidos por un ordenador”. (Comité Internacional Geneve, 2010).

De otro lado Laurent Gisel (2013) asesor legal del Comité Internacional de la Cruz Roja sostiene que:

“Los términos como “ataques cibernéticos” “operaciones cibernéticas” o “ataques contra las redes informáticas” no tienen un significado jurídico acordado a nivel internacional y se usan en diferentes contextos (no siempre vinculados con conflictos armados) y con distintos significados.”

Así, Schmitt (2002) afirma que “Los ataques a través de redes informáticas (ARI), que pueden considerarse como guerra de la información o como simples operaciones de información, son acciones destinadas a “perturbar, rechazar,

deteriorar o destruir la información contenida en ordenadores o en redes informáticas, o los propios ordenadores y redes informáticas."

Los ataques informáticos, son ataques que se realizan a través de las redes informáticas entre ellos tenemos los virus, los cuales son regulados por cada Estado en su normativa interna al no tener de contexto un conflicto armado no se puede aplicar el Derecho Internacional sino el Derecho Interno de cada Estado. Estos ataques informáticos pueden generar un daño irreparable y estos afectar a todo el Estado, entre los ataques cibernéticos más importantes y peligrosos que existen son El Stuxnet y el Flame.

4.1.1 **Stuxnet**

Existen virus informáticos que se propagan por todas las redes, sin identificar entre combatiente y población civil. Este es el caso del virus Stuxnet el cual es un gusano informático que apunta a los sistemas industriales de control que utilizan para controlar instalaciones industriales como plantas de energía eléctrica, represas, sistemas de procesamiento de desechos entre otras operaciones industriales.

Según IEEE Spectrum (2013): "El reconocimiento de este tipo de amenazas estalló en junio de 2010 con el descubrimiento de Stuxnet, un gusano informático de 500 kb que infectó el software de al menos 14 plantas industriales en Irán, incluyendo una planta de enriquecimiento de uranio. A pesar de que un virus informático se basa en una víctima involuntaria de instalarlo un gusano se propaga por sí mismo, a través de una red informática."

"Ese sistema fue capaz de atacar las centrifugadoras de uranio de Irán. Qué podría hacer un sistema similar si atacase aeropuertos, imagínese el caos aéreo.

Que podría hacer si atacase hospitales, modificar todas las fichas o cambiar los sistemas de suministro de medicamente" (Camacho, 2013)

Según Sánchez, G.(2012) menciona "Así, Stuxnet ya es considerado como la mejor arma cibernética jamás creada, al haber dejado fuera de combate a un 20% de las centrifugadoras. Téngase en cuenta que Israel siempre se ha mostrado contraria a la proliferación de este tipo de armamento entre el resto de países de la región, al considerarlo que amenaza su propia existencia como país. Por eso ha hecho todo lo que ha estado en su mano para impedir este desarrollo. Incluso ha llevado a cabo ataques aéreos preventivos por sorpresa contra reactores nucleares en Irak, Siria, Sudán, etc. El problema es con Irán, porque su ruta área es mucho más larga. Además deberían sobrevolar naciones neutrales y, encima, sus instalaciones de enriquecimiento se encuentran bajo tierra. Una operación militarmente posible pero que podría tener más coste que beneficio, dado el riesgo operativo y el coste político. Por tanto, Stuxnet se ha convertido en un arma casi perfecta. En primer lugar, ha provocado daños en las centrifugadoras, como han reconocido los propios iraníes, con todo lo que ello supone para la carrera nuclear que está llevando a cabo Irán: bloqueo y retraso. En segundo lugar, la creación de este troyano habría llevado seis meses para un equipo de cinco personas, por lo tanto, estamos hablando de unos costes muy bajos para un Estado. Y en tercer lugar, puede alcanzar unos objetivos que son invulnerables por otros medios, y además el uso de esta ciberarma no limita el empleo simultáneo de tácticas más convencionales. De ahí que no sea de extrañar que en futuro muy próximo se utilicen ciberarmas como alternativa a las operaciones militares clásicas. Es más, ya tenemos una nueva versión del patógeno gusano, al que los expertos en seguridad han denominado "Duqu", un

virus que está diseñado para robar la información necesaria para organizar un ataque como el llevado a cabo por su predecesor.”

Por el momento esta ciberarma no ha sido utilizado en el contexto de un conflicto armado, en el caso de que esta arma se utilice esta puede generar daños irreparables a la población civil y a los bienes civiles.

4.1.2 Flame

El Flame fue identificado en mayo de 2012 por Kaspersky Lab, MAHER (el Equipo de Respuesta ante Emergencias Informáticas de Irán) y el CrySyS Lab de la Universidad de Tecnología y Economía de Budapest cuando la Unión Internacional de Telecomunicaciones pidió a Kaspersky Lab que investigara unos informes sobre un virus que estaba afectando a los ordenadores del Ministerio del Petróleo de Irán. Mientras Kaspersky investigaba, encontraron un hash MD5 y un nombre de archivo que solo aparecía en ordenadores de Oriente Medio. Después de descubrir más piezas, los investigadores nombraron al programa como "Flame”.

Valenzuela J. (2012) en el diario El País menciona que “El Flame, según informa Douglas Rushkoff en su artículo The cyberwar may be headed to your computer, en CNN, “tiene todos los indicios de constituir un ciberataque maquinado por un Estado nación: es poderoso y complejo y apunta directamente a una zona caliente, Irán”. Su objetivo parece ser sabotear el programa nuclear iraní, pero en los pocos días que lleva bautizado ha provocado un intenso debate entre los especialistas sobre la posibilidad de que se convierta en una peste incontrolable que termine afectando a servicios civiles naciones enteros como redes eléctricas, industrias energéticas, redes bancarias o sistemas de tráfico aéreo.”

Esto quiere decir que es utilizado como un arma dentro de un conflicto armado, la situación puede ser incontrolable y generar efectos que el Derecho Internacional Humanitario prohíbe.

4.2 La ciberguerra

Un ataque cibernético se puede realizar en tiempo de paz o en tiempo de conflicto armado y es ahí donde al conflicto realizado en el ciberespacio se le denomina "ciberguerra". Dentro de la ciberguerra el Estado va a tener responsabilidad siempre y cuando el ataque cibernético esté relacionado con el Estado (nexo). No es necesario que el Estado planifique todas las operaciones de las unidades dependientes, elija sus objetivos, o de instrucciones específicas sobre la conducción de las operaciones militares y las presuntas violaciones de Derecho Internacional Humanitario. Basta que el Estado tenga un papel de organización, coordinación o planificación de las acciones militares del grupo militar además de financiamiento, capacitación y equipamiento para realizar la operación.

Dentro de un conflicto armado se entiende por "ataque" según Verri P. (2008) "En el sentido del derecho internacional, el ataque es un acto de violencia cometido contra el adversario, cuyo objetivo es tanto ofensivo y defensivo e independientemente del territorio sobre el cual se lleva a cabo."

¿Qué es la ciberguerra? Es la pregunta que todos nos hacemos al principio. Según Laurent Gisel (2013) asesor legal del Comité Internacional de la Cruz Roja, en la entrevista brindada a su institución sostiene que:

> "Cuando hablamos de guerra cibernética, nos referimos solamente a los medios y los métodos bélicos que consisten en operaciones cibernéticas

que alcanzan el nivel de un conflicto armado o son conducidas en el contexto de un conflicto armado, según los términos del Derecho Internacional Humanitario.

El concepto de guerra cibernética es un tanto impreciso y, al parecer, su significado varía según quién lo use. En el marco de este debate, a diferencia de las tradicionales operaciones militares cinéticas, la guerra cibernética se refiere a los medio y métodos de guerra que se basan en la tecnología de la información y se usan en el contexto de un conflicto armado en el sentido del derecho internacional humanitario."

"La guerra de la información es, en pocas palabras, un subconjunto de operaciones de información que pueden definirse como "las acciones que se realizan para alterar la información y los sistemas de información del adversario, mientras se protege la información y los sistemas de información propios". (Schmitt, M.N., 2002)

¿Qué normativa es aplicable a la ciberguerra? Si hablamos de una ciberguerra (entiéndase ataques informáticos dentro de un conflicto armado) se debe aplicar el Derecho Internacional Humanitario; según Cordula Droege (2011) asesora legal del Comité Internacional de la Cruz Roja (CICR) en la entrevista brindada a su institución sostiene que:

"El Derecho Internacional Humanitario o DIH sólo entra en juego si las operaciones cibernéticas se cometen en el contexto de un conflicto armado, sea entre Estados, entre Estados y grupos armados organizados, o entre grupos armados organizados. Por ende, es preciso distinguir la

cuestión general de seguridad cibernética, de la cuestión específica que representan las operaciones cibernética en un conflicto armado."

El problema que surge en este caso es saber si la normativa del Derecho Internacional Humanitario es adecuada para prevenir o limitar estos ataques. Schmitt (2002) llegó a la conclusión de que :

> "… las normas prescriptivas existentes de derecho humanitario son suficientes para conservar la protección de que gozan las personas civiles, de los bienes de carácter civil y de otras personas jurídicas.
>
> El mero hecho de que un objetivo pueda ser "atacado" por un medio no cinético no significa que las normas de derecho humanitario sean inaplicables. Las personas civiles y los bienes de carácter civil siguen gozando de un estatuto de protección contra los aspectos de los ataques de redes informáticas que causen sufrimiento humano y daños físicos."

Si bien es cierto el DIH prevé los ataques indiscriminados a la población y bienes civiles pero muchas veces no son lo suficientemente necesarios para lograr su objetivo; por ello es necesaria la regulación específica de determinadas armas.

El Comité Internacional de la Cruz Roja (2010) resalta que "La guerra informática añade un nuevo nivel de complejidad a los conflictos armados que puede conllevar nuevas cuestiones para el DIH. Por ello, debe reafirmarse la pertinencia del DIH como el principal ordenamiento jurídico que regula ese tipo de guerras. Las normas de Derecho Internacional Humanitario que abarcan cuestiones como el empleo de armas indiscriminadas, la distinción entre objetivos militares y bienes de carácter civil, la proporcionalidad y la perfidia, pueden y deben aplicarse también a la guerra informática."

“El DIH no menciona concretamente las operaciones cibernéticas. Por esta razón y porque la explotación de la tecnología cibernética es relativamente novedosa y, en ocasiones, parece introducir un cambio cualitativo completo en los medios y métodos de guerra, en algunos casos se ha señalado que el DIH no está adaptado a este ámbito y no puede aplicarse a la guerra cibernética. No obstante, el hecho de que el DIH no contenga referencias específicas a las operaciones cibernéticas no significa que esas operaciones no estén sujetas a sus normas. Si los medios y métodos de la guerra cibernética producen los mismos efectos en el mundo real que las armas convencionales (destrucción, desorden, daños, lesiones o muerte), se rigen por las mismas normas que las armas convencionales.” (Cordula Droege, 2011)

En conclusión, la guerra cibernética o ciberguerra son ataques informáticos que se desarrollan dentro de un conflicto armado nacional o internacional y ello genera la aplicación del Derecho Internacional Humanitario. Los ataques cibernéticos que no se desarrollan dentro de un conflicto armado; por ende, no son parte de una ciberguerra, sino son simples ataques informáticos que se regulan por la normativa interna de cada Estado.

CAPITULOO V

Los ciberataques a la luz de los principios del derecho internacional de los conflictos armados

En el presente capítulo se desarrollará los principios más relevantes del Derecho Internacional Humanitario los cuales pueden ser afectados en el caso de una ciberguerra.

Desde la costumbre desarrollada anteriormente por diferentes culturas se tenía en claro muchos principios, los cuales no eran reconocidos por todas las civilizaciones. Ello hizo que posteriormente se llegue a una codificación de sus costumbres y estas se vuelvan normas imperativas.

Al analizar varios de sus principios, nos daremos cuenta si realmente el Derecho Internacional Humanitario se encuentra acorde a la evolución de la tecnología y

si está preparado para enfrentar estos nuevos retos o si se necesita la creación o modificación de un instrumento internacional.

5.1 Principio de distinción

El principio de distinción es uno de los principios claves del Derecho Internacional Humanitario y es sumamente necesario su respeto dentro de las operaciones militares en los conflictos armados. Este principio se aplica a los combatientes y no combatientes, y entre los objetivos militares y bienes civiles.

“El propósito de esta diferenciación es que las hostilidades se libren entre combatientes y contra objetivos militares para que en ninguna circunstancia afecten a los no combatientes y a los bienes civiles. Es lícito atacar pues a un combatiente y a un objetivo militar como es ilícito atacar a un no combatiente y a un bien civil.” (Valencia, A., 2013, p.157)

Según Schmitt, M. (2002) señala que “El principio de distinción, que es sin duda alguna parte del derecho humanitario consuetudinario, está establecido en el artículo 48 del Protocolo adicional I: Las partes en conflicto harán distinción en todo momento entre la población civil y combatientes, y entre bienes de carácter civil y objetivos militares y, en consecuencia, dirigirán sus operaciones únicamente contra objetivos militares. Mientras la prohibición de los ataques directos contra personas civiles deja fuera de su alcance a una categoría especifica de objetivos potenciales, el requisito de distinción extiende la protección casos en los que un ataque puede no dirigirse específicamente contra personas civiles o bienes de carácter civil, pero cuya probabilidad de alcanzarlos es, sin embargo, muy elevada. Un ejemplo sería disparar un arma a ciegas, aunque sea posible dirigirla contra un blanco.”

Para una explicación mejor Salmòn E. (2012) manifiesta que “El principio de distinción sintetiza, a su vez, otros principios que regulan los ataques, a saber: el objetivo militar, el principio de proporcionalidad y el principio de necesidad militar. El objetivo militar significa que solo se podrá atacar bienes que por su naturaleza, ubicación, finalidad o utilización contribuyan eficazmente a la acción militar y cuya destrucción total o parcial, captura o neutralización, ofrezcan una ventaja militar definida. El concepto es relativo en sí mismo ya que un bien puede revestir la característica de objetivo militar y luego abandonarla o viceversa. En caso de duda cerca de si un bien que normalmente se dedica a fines civiles se utiliza para contribuir eficazmente a la acción militar, se presumirá que no se utiliza con tal fin.” (p. 59)

Para poder entender el principio de distinción es necesario estudiarlo de manera amplia y conforme las normas y costumbres del Derecho Internacional Humanitario*.*

a) ***Las partes en conflicto deberán distinguir en todo momento entre personas civiles y combatientes. Los ataques sólo podrán dirigirse contra combatientes. Los civiles no deben ser atacados.***

El principio de distinción no admite ninguna clase de reserva ya que estás serían incompatibles con su objetivo y fin. En el Estatuto de la Corte Penal Internacional (CPI) se detalla que “dirigir intencionalmente ataques contra la población civil en cuanto tal o contra civiles que no participan directamente en las hostilidades” constituye un crimen de guerra en los conflictos armados internacionales.

“La Corte Internacional de Justicia en su opinión consultiva en relación con las armas nucleares, declaró “que el principio de distinción era uno de los “principios

cardinales" del derecho internacional humanitario y uno de los "principios inviolables del derecho internacional consuetudinario". (CIJ, Nuclear Weapons case, opinion consultiva, parr.434).

El Tribunal Penal Internacional para la ex Yugoslavia, en particular en los asuntos Tadic, Martic y Kupreskic, y de la Comisión Interamericana de Derechos Humanos en el asunto relacionado con los acontecimientos de la Tablada en Argentina, proporcionan pruebas de que existe obligación de hacer la distinción entre civiles y combatientes por derecho consuetudinario, tanto en los conflictos armados internacionales como no internacionales.(párrs. 443 y 810)

b) Quedan prohibidos los actos o las amenazas de violencia cuya finalidad principioal sea aterrorizar a la población civil.

Esta norma está regulada en el artículo 51, párrafo 2, del Protocolo adicional I; los actos de violencia dirigidos a la población civil se encuentran prohibidos por esta norma, inlcuyen el apoyo ofensivo o las operaciones de ataque destinadas a sembrar el terror en la población civil,el fuego masivo e indiscriminado y los bombardeos sistemáticos de ciudades. Hay que resaltar que esta norma está respaldada por el IV Convenio de Ginebra específicamente en el artículo 33. De igual manera se encuentra plasmado en el artículo 13 párrafo 2 del Protocolo Adicional II prohíbe los actos o amenazas de violencia cuya finalidad principal sea aterrorizar a la población civil.

Henckaerts, J-M. & Doswald-Beck, L (2007) afirman que "Puede aducirse que la prohibición de los actos o las amenazas de violencia que tienen por objeto aterrorizar a la población civil está, además, respaldada por la prohibición más amplia de "los actos de terrorismo" en el artículo 4, párrafo 2, del Protocolo adicional II. Los "actos de terrorismo" están tipificados como crímenes de guerra en el Estatuto del Tribunal

Penal Internacional para Rwanda y del Tribunal Especial para Sierra Leona. En su ifnorme sobre el establecimiento de un Tribunal Especial para Sierra Leona, el Secretario General de las Naciones Unidas señaló que las violaciones del artículo 4 del Prtocolo adicional II eran consideradas desde hacía tiempo como crímenes según el derecho internacional consuetudinario". (p.11).

c) ***Todos los miembros de las fuerzas armadas de una parte en conflicto son combatientes, excepto el personal sanitario y religioso.***

Rodriguez-Villasante y Prieto, (2009), afirman que "El DIH contemporáneo nació en 1864 para proteger a los heridos y enfermos de las fuerzas armadas en campaña. En el primer Convenio de Ginebra de 22 de agosto de 1864 ya se hacía referencia a la obligación de respetar y proteger al personal sanitario, que participa del estatuto de neutralidad, que concedía esta norma internacional mientras estén ejerciendo sus funciones y si caían en poder de la parte adversaria quedarían exentos de captura, permitiendoles el regreso a su ejercito. Así desde los orígenes, el DIH protege al personal sanitario".(p.4).

Por ello se concluye que el personal sanitario y religoso se les considera como no combatientes aun siendo de las fuerzas armadas.

d) ***Las fuerzas armadas de una parte en conflicto se compoonen de todas las fuerzas agrupaciones y unidades armadas y organizadas que estén bajo un mando responsable de la conducta de sus subordinados ante esa parte.***

Esta norma se encuentra regulada en el párrafo 1 del artículo 43 del Protocolo adicional I. La definición de fuerzas armadas tienen su origen en el articulo 3 del

Reglamento de La Haya (1907) y en el III Convenio de Ginebra de 1949. Para tener la calidad de combatiente, en el Reglamento de La Haya (1907) se encuentran algunas condiciones que tenían que cumplirse. Actualmente dichas condiciones han sido reducidas sin alterar sustancialmente la definición de fuerzas armadas que sirve para determinar qué combatientes tienen derecho al estatuto de prisionero de guerra.

e) Son personas civiles quienes no son miembros de las fuerzas armadas. La poblacion civil comprende a todas las personas civiles.

Esta norma se encuentra regulada en el artículo 50 del Protocolo adicional I para los conflictos internacionales; hay que resaltar que en el Protocolo adicional II no contiene una definición de población civil a pesar de que expresión se usa en varias disposiciones.

Según Henckaerts & Doswald-Beck (2007), “En la práctica de los Estados se añade, a veces, la condiciòn de que los civiles son personas que toman parte en las hostilidades. Este requisito adicional unicamente refuerza de que una persona civil que participa directamente en las hostilidades pierde la protección contra los ataques”. (p.20)

Si bien es cierto los Estados no han hecho reserva alguna a la norma, encontramos una excepción, la cual es el levantamiento en masa. Los habitantes de un país que aún no ha sido ocupado toman espontáneamente las armas, cuando se aproxima el enemigo, para oponerse a las tropas invasoras, sin tener tiempo para organizarse en una fuerza armada,estas personas son consideradas combatientes si llevan las armas a la vista y respetan las leyes y constumbres de la guerra. Esta es la unicá excepción que hasta el momento se ha encontrado en el principio distinción. (III Convenio de Ginebra de 1949, art. 4, Letra A, parr.6)

f) Las personas civiles gozan de protección contra los ataques, salvo si participan directamente en las hostilidades y mientras dure tal participación.

Esta norma está contenida en el artículo 51, párrafo 3 del Protocolo adicional I y en el artículo 13 del Protocolo adicional II.

Según la Comisión Interamericana de Derechos Humanos, en el caso de la Tablada – Argentina, estimó que los civiles que participan directamente en los enfrentamientos, ya sea solos o como parte de un grupo, se convierten en objetivos militares legítimos, pero sólo mientras participen activamente en los combates. De igual modo la Comisión emitió el tercer informe sobre los derechos humanos en Colombia en el cual afirmó que la expresión "participación directa en las hostilidades" se entiende, en general, "actos que por su índole o finalidad tiene por objeto causar efectivamente daño al personal o material del enemigo."

En el caso de que exista duda entre civil y combatiente, el Protocolo adicional I en su artículo 50 ha intentado resolver esta cuestión disponiendo que en caso de duda acerca de la condición de una persona, se la considerará como civil.

5.2 Principio de Proporcionalidad

El principio de proporcionalidad no se encuentra codificado de manera específica en la normativa del Derecho Internacional Humanitario. Pero podemos encontrarlo de manera indirecta en el artículo 51, párrafo 5, apartado b) del Protocolo adicional I de los Convenios de Ginebra de 1949.

Según Valencia (2013), en el artículo 57.2.a) iii) del Protocolo I de 1977 enuncia la regla de la proporcionalidad al establecer que quienes preparen o decidan un ataque deberán abstenerse de decidir un ataque cuando sea de prever que

causará incidentalmente muertos o heridos en la población civil, daños a bienes de carácter civil, o ambas cosas, que serían excesivos en relación con la ventaja militar concreta y directa prevista. De igual manera analiza que este principio no solo abarca los daños que pueden causar a los civiles y/o bienes civiles sino que también a los combatientes ya que en sí hace un estudio de los parámetros de los daños que se originan dentro de un conflicto armado. Es importante resaltar que el principio de proporcionalidad está unido a los demás principios y sobre todo muy anexado al principio de limitación. (p.222)

El Comité Internacional de la Cruz Roja (2010) afirma que todo el derecho de los conflictos armados es el resultado de un justo equilibrio entre las necesidades de la guerra y los imperativos humanitarios. No existe en los Convenios ninguna cláusula sobrentendida que dé prioridad a las exigencias militares. El objeto de los principios de estos Convenios es precisamente fijar el límite y el principio de proporcionalidad contribuye a ello.

El Estatuto de la Corte Penal Internacional en su artículo 8 párrafo 2 menciona que lanzar un ataque intencionalmente, a sabiendas de que causará perdidas incidentales de vidas, lesiones a civiles o daños a bienes de carácter civil (…) que serían manifiestamente excesivos en relación con la ventaja militar concreta y directa de conjunto que se prevea" constituye un crimen de guerra en los conflictos armados internacionales.

"En cualquier caso, cuando se atacan objetivos militares debe respetarse además el principio de proporcionalidad que exige que la afectación a bienes y personas civiles sea menor a la ventaja militar que se busca obtener. En efecto, cuando son atacados objetivos militares, las personas civiles y los bienes de carácter civil deben preservarse lo más posible de daños incidentales y estos

además no deben ser excesivos con respecto a la directa y concreta ventaja militar esperada de cualquier ataque contra un objetivo militar." (Salmón, E., 2012, p.60)

Según Henckaerts & Doswald-Beck (2007) "el Protocolo adicional II no contiene ninguna referencia explícita al principio de proporcionalidad en el ataque, pero se ha sostenido que es inherente al principio de humanidad, el cual se hizo explícitamente aplicable al Protocolo en su preámbulo y que, por ello, no puede ignorarse el principio de proporcionalidad en la aplicación del Protocolo." (p.55)

Menciona el Comité Internacional de la Cruz Roja en la XXVIII Conferencia Internacional de la Cruz Roja y de la Media Luna Roja que "La desproporción entre, por un parte, las pérdidas civiles y los daños causados a los civiles, y por otra parte a la ventaja militar prevista, plantea un delicado problema: en algnas situaciones no hay lugar a dudas, mientras que en otras pueden haber razones para vacilar. En tales situaciones complejas, deben prevalecer los intereses de la población civil. Se debe tener en cuenta que el derecho internacional humanitario exige que constantemente se tenga cuidado de preservar a la población civil, a los civiles y a los bienes de carácter civil. No hay que olvidar que incluso ataques que podrían ser lícitos, es decir, ajustados a la regla de la proporcionalidad y a otros principios jurídicos, pueden causar, a pesar de todo, sufrimiento enorme entre los civiles." (p. 13)

También es bueno recordar que en la jurisprudencia del Tribunal Penal Internacional para la ex Yugoslavia en el caso Martic y en el tercer informe de derechos humanos en Colombia de la Comisión Interamericana de Derechos Humanos proporcionan pruebas de que esta norma es consuetudinaria en los conflictos armados no internacionales.

Por ultimo “Esta norma es válida cuando el arma empleada es lícita desde el principio y el blanco del ataque es un objetivo militar según la definición que de él se da en el derecho humanitario. En la norma se prohíbe que se lleve a cabo un ataque de este tipo si se prevé que las víctimas colaterales serán excesivas con respecto al valor del objetivo militar.” (Dosvvald-Beck, L., 1997, p. 46)

5.3 Principio de limitación

Este principio está dirigido a la utilización de los medios y métodos de combate ya que no es ilimitado su uso. El Protocolo Adicional I a los Convenios de Ginebra recoge este principio en el artículo 35 en los siguientes términos:

> *“1.- En todo conflicto armado, el derecho de las Partes en conflicto a elegir los métodos o medios de hacer la guerra no es ilimitado.*
>
> *2.- Queda prohibido el empleo de armas, proyectiles, materias y métodos de hacer la guerra de tal índole que causen males superfluos o sufrimientos innecesarios.*
>
> *3.- Queda prohibido el empleo de métodos o medios de hacer la guerra que hayan sido concebidos para causar, o de los que quepa prever que causen, daños extensos, duraderos y graves al ambiente natural.”*

Según Valencia (2013) “este principio comprende dos tipos de normas fundamentales, por un lado, normas humanitarias y, por otro, normas de lealtad. Las normas humanitarias prohíben dar muerte o herir a un enemigo que, habiendo depuesto las armas o no teniendo ya medios de defenderse, se haya entregado, así como negarse a dar cuartel y causar males superfluos. Las normas de lealtad prohíben dar muerte o herir a traición, así como engañar al enemigo con el uso abusivo de la bandera blanca, de emblemas nacionales o de

uniformes del enemigo o también hacer uso indebido del signo de la Cruz Roja. Toda potencia militar sin excepción debe incluir estos principios fundamentales en las instrucciones impartidas a sus tropas". (p. 204)

Para entender este principio debe determinarse las palabras "superfluos e innecesarios" y cómo han de medirse los "males o sufrimientos". Para ello debemos tomar diversas normativas del Derecho Internacional Humanitario.

Por ello, Salmón, E., (2012) menciona que "El principio de limitación establece que el derecho a elegir los métodos y medios de combate no es ilimitado, sino que deben atenderse a razones humanitarias. De este mismo principio se deriva el de prohibición de causar daños suplerfluos o sufrimientos innecesarios, que tiene por finalidad prohibir las armadas pensadas para ocasionar efectos innecesarios en relación con el fin de dejar a los enemigos fuera de combate. Otro principio ligado a los anteriores antes enunciados, consiste en la protección del medio ambiente natural. El principio deriva del carácter limitado de la elección de los métodos de combate por las partes y, partiendo del hecho de que del hecho de que todo conflicto armado daña el medio ambiente natural, se busca impedir que se utilice la destrucción de este como método de combate." (p.61)

Es "un factor importante a la hora de establecer si un arma pueda causar males superfluos o sufrimientos innecesarios es que no pueda evitarse una discapacidad grave permanente." (Henckaerts & Doswal-Beck, 2007, p. 269)

"Se deben diferenciar las armas cuyo empleo es absolutamente necesario para la seguridad de las partes, y aquellas cuyo empleo puede ser simplemente útil desde el punto de vista militar. Es necesario sopesar esta utilidad militar en relación con el sufrimiento causado, y cuando éste es grave, debe demostrarse

que aquélla es también importante. Se prohíbe la utilización indiscriminada del arma pero no el arma como tal." (Valencia, 2013, p.207)

Por ultimo según el profesor chileno Salinas Burgos, el principio de limitación ante todo da pie a una reglamentación de los medios y métodos de combate entre las partes beligerantes, ya que en última instancia desconoce, pues, una necesidad militar absoluta que pudiese llegar a justificar el empleo de medios y métodos libres e indiscriminados, o que excedan el propósito expreso de la ventaja militar particular.

5.4 Principio de Necesidad Militar

Este principio se encuentra en el Preámbulo de la Declaración de San Petersburgo de 1868 en el cual menciona "el único objetivo legítimo que los estados deben proponerse durante la guerra es la debilitación de las fuerzas militares del enemigo". De igual manera lo encontramos en el artículo 23(g) del Reglamento de La Haya de 1907, según el cual está prohibido "destruir o apoderarse de las propiedades enemigas, excepto en el caso en que estas destrucciones o apropiaciones sean imperiosamente reclamadas por las necesidades de la guerra."

Según el Comité Internacional de la Cruz Roja (2001) aunque el principio es claro, las nociones que abarca requieren algunas explicaciones. El derecho de los conflictos armados es una solución de avenencia fundada en un equilibrio entre las necesidades militares, por una parte, y las exigencias de humanidad, por otra. Habitualmente se expresa en forma de prohibiciones que tienen ya en cuenta la necesidad militar. Por necesidad militar se entiende la necesidad de medidas indispensables para lograr los objetivos bélicos, medidas que son legales según las leyes y costumbres de la guerra. Por consiguiente, no se puede

suspender una norma del derecho de los conflictos armados incoando la necesidad militar más que cuando tal posibilidad está explícitamente prevista por la norma en cuestión. Inversamente, cuando el derecho de los conflictos armados no prevé prohibición alguna, las partes en conflicto son en principio libres, dentro de las limitaciones del derecho consuetudinario y de los principios generales. (p. 550)

El principio de necesidad militar, según Novak, F. & otros (2003) señalan que también “es llamado principio del debilitamiento bélico del adversario, permite solamente a los combatientes debilitar o destruir el potencial bélico de su contendor, de forma que no se causen daños desproporcionados al objetivo que se persigue”. (p. 135)

Este principio se encuentra ligado con el principio de proporcionalidad, como señala Salmon, E. (2004) el principio de necesidad militar justifica aquellas medidas de violencia militar que son necesarias y proporcionadas para garantizar el rápido sometimiento del enemigo con el menor costo posible en vidas humanas y recursos económicos. Es decir que en el transcurso de las operaciones militares solo se deben tomar las medidas necesarias para obtener el objetivo propuesto. (p.56)

“El derecho Internacional Humanitario exige de quienes participan en las hostilidades una serie de requisitos tales como organización, estrategia militar, ataques meditados y sustentados, y descartarse, cuando menos evitarse, los errores e improvisaciones.” (Novak, F. 2003, p. 135)

5.5 Principio de Humanidad

El Principio de Humanidad señala Novak F. (2003) que "también es llamado principio de los no combatientes, enuncia que las personas puestas fuera de combate y aquellas que no participan directamente en las hostilidades serán respetadas, protegidas y tratadas con humanidad; vale decir, establece ciertas condiciones indispensables que aseguran para los individuos que ya no participan activamente en el enfrentamiento, un trato aceptable, acorde con su calidad de ser humano. Lo mismo ocurre con quienes se dedican a la asistencia humanitaria, sea esta sanitaria, médica, de socorro o religiosa. Su actuación nunca constituye una injerencia, toda vez que se encuentran impedidos de participar en las hostilidades y su accionar se limita al servicio que ofrecen." (p. 133)

De igual manera "El principio de protección, también denominado de humanidad o de inmunidad, establece que la población civil, los heridos, los enfermos y las personas puestas fuera de combate serán protegidas, tratadas de manera humana y que son inmunes, es decir, que no deben ser atacadas mientras no participen directamente en las hostilidades." (Valencia, 2013, p. 238)

Según Salmón, E. (2010) "el principio de humanidad consiste en respetar y tratar a todas las personas con humanidad, tanto a los combatientes, a quienes no se les hará padecer sufrimientos innecesarios, como a los no combatientes, quienes en todo momento deberán ser tratados con humanidad. Es decir que mientras, el principio de distinción separa a los que combaten de los que no, el principio de humanidad los une en una misma protección." (p.54)

5.6 Principio de Protección al Medio Ambiente

Este principio intenta regular los efectos que producen las armas al ambiente. Según Salmón, E. (2003) "la degradación del medio ambiente apareció como tema de interés en el ámbito internacional hacia fines de la década de 1960, pero el factor detonante para su inclusión en el marco del DIH fue la deforestación a gran escala llevada a cabo durante la guerra de Vietnam como método de combate. Este principio deriva del carácter limitado de la elección de los métodos de combate por las partes y, partiendo del hecho de que todo conflicto armado daña el medio ambiente natural, se busca impedir la utilización de la destrucción de este como método de combate." (p. 58)

Este principio es de mucha importancia ya que es relevante para determinar los medios y métodos de combate. Actualmente contamos con Directrices para la Protección del Medio Ambiente en Tiempo de Conflicto Armado en la cual se prohíbe que la modificación deliberada del medio ambiente para infligir daños extensos, duraderos o graves como medio para causar destrucción, daños o perjuicios a otro Estado Parte se encuentra prohibido.

El Comité Internacional de la Cruz Roja (2001) menciona que "la noción del medio ambiente natural ha de entenderse en su acepción más amplia, que abarca el medio biológico en el que vive una población. No se trata aquí solamente de los bienes indispensables para la supervivencia de la población sino, además, de los bosques y otros tipos de cubierta vegetal, citados en la Convención del 10 de octubre de 1980 sobre Prohibiciones o Restricciones del Empleo de Ciertas Armas Convencionales, así como de la fauna, la flora y otros elementos biológicos o incluso climáticos." (p. 924)

Como señala CIJ en su Opinión Consultiva sobre la Legalidad o el Empleo de Armas Nucleares, señala que los Estados no poseen un derecho ilimitado a escoger los medios ni los métodos de combate dentro de un conflicto armado, sino que aquellos se encuentren vinculados por razones humanitarias que efectivamente los limitan.

5.7 ¿Son incompatibles los principios del Derecho Internacional Humanitario con los ataques cibernéticos?

Para determinar si los principios del Derecho Internacional Humanitario son compatibles con la ciberguerra ha sido necesario el estudio de ellos. Una vez concluidos podemos determinar lo siguiente:

- ✓ El principio de distinción es uno de los principios cardinales del Derecho Internacional Humanitario, reconocido por la Corte Internacional de Justicia en su Opinión Consultiva sobre la Legalidad de la amenaza o empleo de armas nucleares, por ende este principio debe ser aplicado y respetado antes del lanzamiento de un ataque. En este caso el principio de distinción puede ser aplicado en el momento de realizar un ataque cibernético entre las fuerzas armadas, pues recordemos que el principio de distinción según el artículo 48 del Protocolo adicional I tiene el fin de garantizar el respeto y protección de la población civil, combatientes, los bienes de carácter civil y distinguir entre objetivos militares y otros bienes. Empero, se concluye que los Estados deben de realizar sus ataques cibernéticos solamente a los objetivos militares, miembros de las fuerzas armadas más no a la población civil y bienes civiles.

El problema radica cuando este ataque que se encuentra dirigido a un objetivo militar y genera daños colaterales que afecta a la población civil o

bienes civiles. Por ejemplo: Si un Estado A dirige un ataque cibernético dentro de un conflicto armado a una determinada infraestructura cibernética que es objetivo militar, pero esta infraestructura afecta una planta de agua, de luz o de centrales de emergencia (hospitales, postas, etc.), los civiles pueden quedar privados de bienes básicos como el agua potable, la atención médica y la electricidad. Estos de igual manera, podían interferir en los servicios de rescate o causar daños a infraestructuras, como las plantas nucleares y sistemas de control aéreo; por eso "De todos modos, no podemos descartar que tal vez sea necesario desarrollar el derecho para que brinde suficiente protección a la población civil, a medida que evolucionan las tecnologías cibernéticas o se comprende mejor su impacto en el plano humanitario." (Laurent, G., 2013)

El ataque cibernético dentro de un conflicto armado debe ser proporcional y necesario. La necesidad siempre es determinada por parte del Estado y la proporcionalidad, según Schmitt, M. & otros (2013/2015) menciona que "el criterio limita la escala, el alcance, la duración y la intensidad de la respuesta defensiva a la que se requiere para poner fin a la situación que ha dado lugar al derecho de actuar en defensa propia." (p.60). Además hay que recordar que un Estado puede lanzar un ataque cibernético dentro de un conflicto armado, siempre y cuando este último no genere daño o amenaza (de manera inminente) a otro Estado y este ataque debe de responder en la misma escala que el anterior y por consiguiente no debe generar mayor impacto en la población civil, en los no combatientes y en las personas o bienes protegidos por el Derecho Internacional Humanitario que el causado por el primer ataque cibernético. Respetando lo dicho anteriormente; solo así

determinaremos que el ataque cibernético dentro de un conflicto armado es proporcional y necesario.

- ✓ El principio de limitación también es un principio importante ya que no se permiten realizar ataques indeterminados bajo ningún arma y método. Los ciberataques solo deben realizar para generar una ventaja contra e adversario, pero esta ventaja no puede tener ataques ilimitados que generen daños colaterales, males superfluos o sufrimientos innecesarios, conforme el artículo 35 del Protocolo Adicional I a los Convenios de Ginebra.
- ✓ El principio de necesidad militar es un principio que se encuentra unido al principio de proporcionalidad. En el caso de un ciberataque, este solo debe ser lanzado cuando otro Estado amenace o realice un ataque determinado y este ataque debe ser solamente dirigido a un objetivo militar.
- ✓ El principio de humanidad si se puede ver vulnerado ya que, como mencione en el ejemplo anterior, los efectos colaterales de un ciberataque pueden dañar a infraestructuras de salud, energía eléctrica y de agua potable, afectando así a la población civil.
- ✓ Por último el principio de protección al medio ambiente, en un primer momento, sí puede ser favorecido. Al efectuar un ataque cibernético este no generaría un impacto ambiental ya que no se usaría ningún químico para realizar el ataque. Pero es relevante mencionar que el impacto ambiental y humanitario se podría generar si este ciberataque es dirigido

a una determinada infraestructura ambiental y este ataque tendría consecuencias en una determinada planta nuclear.

A manera de conclusión se puede decir que los principios del Derecho Internacional Humanitario son aplicables para los ciberataques dentro de un conflicto armado, pero no siempre estos limitarán su uso. Por ello es necesario que se desarrolle una normativa internacional específica para los ataques cibernéticos dentro de los conflictos armados y esta normativa debe estar basada en la ya existente por el Derecho Internacional Humanitario. De igual manera es importante que cada Estado cuente con un “Plan Estratégico de ciberseguridad” y con una oficina de Dirección para Operaciones Cibernéticas para que puedan estar preparados para en caso se desarrolle una ciberguerra.

CAPITULO VI

Análisis de la ciberguerra conforme el artículo 36 del Protocolo Adicional I

Se considera un capítulo específico para el análisis del artículo 36 del Protocolo Adicional I de los Convenios de Ginebra ya que obliga a todos Estados a realizar un examen jurídico de las nuevas armas, medios y métodos de guerra; esto quiere decir que el Estado antes de realizar un ataque mediante cualquier medio "nuevo" o no regulado por el Derecho Internacional Humanitario este debe realizar un examen jurídico para saber si esta arma o medio de ataque es compatible con el Derecho Internacional Humanitario.

El presente capitulo abordara este tema y al finalizarlo realizará un análisis para saber si un ciberataque es compatible con el Derecho Internacional Humanitario.

6.1 Examen Jurídico de las nuevas armas fundamentado en el artículo 36 del Protocolo adicional I.

El Articulo 36 del Protocolo Adicional I menciona: “Cuando una Alta Parte Contratante estudie, desarrolle, adquiera o adopte una nueva arma, o nuevos medios o métodos de guerra, tendrá la obligación de determinar si su empleo, en ciertas condiciones o en todas las circunstancias, estaría prohibido por el presente Protocolo o por cualquier otra norma de derecho internacional aplicable a esa Alta Parte Contratante.”

Según el Comité Internacional de la Cruz Roja (2006) “La finalidad del artículo 36 es prevenir el empleo de armas que violarían el derecho internacional en todas las circunstancias e imponer restricciones el empleo de armas que violarían el derecho internacional en algunas circunstancias, determinando su licitud antes de que sean desarrolladas, adquiridas o incorporadas de alguna otra manera al arsenal de un Estado.” (p. 4)

El artículo 36 bien menciona que cada Estado debe de determinar la licitud de las armas y métodos que van a utilizar. Pero no es necesario que dicha evaluación de la licitud sea revelada. El CICR (2001) señala que “esta reserva es comprensible, ya que la estrategia moderna no se basa con mucha frecuencia en las maniobras clásicas del arte militar, sino en esta nueva posibilidad, que proporcionan la investigación y los estudios, consistente en crear un desequilibrio en el adversario utilizando precisamente una superioridad tecnológica que se concreta en nuevas armas.” (p.503)

En 1999 la XXVII Conferencia Internacional de la Cruz Roja y de la Media Luna Roja alentó a los Estados a establecer mecanismos y procedimientos, para el empleo de las armas, ya sea las mantenidas en sus arsenales o las que se

adquieren o se desarrollan. De igual manera en el año 2003 la XXVIII Conferencia Internacional de la Cruz Roja y de la Media Luna Roja reafirmó el objetivo de garantizar la licitud de las nuevas armas de conformidad con el Derecho Internacional y afirmo que todos los métodos y medios nuevos de ataque deberán someterse a exámenes rigurosos y multidisciplinarios.

Esta obligación es para los Estados productores y compradores de armas. Los Estados compradores se encuentran en la obligación de realizar este examen antes de adquirir cualquier tipo de arma, sobre todo si es parte de la Convención sobre Prohibiciones o Restricciones del Empleo de Ciertas Armas Convencionales que Puedan Considerarse Excesivamente Nocivas o de Efectos Indiscriminados, de ello se determinará si su adquisición y posteriormente su utilización del arma o método es compatible con el Derecho Internacional Humanitario. Los Estados productores, desde que son parte del Protocolo adicional I el artículo 36 los obliga al igual que los compradores, pero no obliga a estos Estado a prohibir la venta de las armas. Lo ideal sería que al igual que el Estado comprador, el Estado productor también tuviera responsabilidad por incentivar a la compra de las armas.

El CICR (2006) señala como los Estados deben de realizar un examen jurídico para saber si un arma o método se encuentra conforme con el Derecho Internacional Humanitario, “El primer paso es determinar si el empleo del arma o el medio de guerra bajo examen está prohibido o restringido por un tratado que vincula al Estado examinador o por el derecho internacional consuetudinario. Si no existe una prohibición específica, el paso siguiente es determinar si el empleo del arma o medio de guerra bajo examen y los métodos normales o previstos con que se utilizarán respetaría las normas generales aplicables a todas las

armas, medios y métodos de guerra que figuran en el Protocolo adicional I y en otros tratado que vinculan al Estado examinador o en el derecho internacional consuetudinario. En ausencia de normas convencionales o consuetudinarias pertinentes, la autoridad examinadora debería considerar el arma propuesta a la luz de los principios de humanidad y los dictados de la conciencia pública." (p. 11)

Para poder cumplir con el Protocolo Adicional I, es necesario que cada Estado cuente con una Comisión Especializada en armas y en Derecho Internacional Humanitario para que pueda realizar la evaluación y el Estado no caiga en responsabilidad internacional. La autoridad que evalúe el arma o medio de combate debe de prestar atención no solo al diseño y a las características del arma, sino que también debe es importante saber cómo será su utilización. Los factores que deben considerarse generalmente son de índole militar, salud, técnica y ambiental; por ende debería estar en la Comisión Especializada expertos jurídicos, militares, ambientales, en salud, en tecnologías de armas para que puedan evaluar la información relativa al arma nueva y puedan tomar una decisión sobre la licitud.

Es importante que cada Estado determine el mecanismo de cada examen, según CICR (2006) "Es responsabilidad de cada Estado adoptar las medidas legislativas, administrativas, reglamentarias y/u otras apropiadas para aplicar efectivamente esta obligación. Como mínimo, el articulo 36 exige que cada Estad Parte establezca un procedimiento formal y, de conformidad con el artículo 84 del Protocolo adicional I, otros Estados Partes en el Protocolo pueden solicitar ser informados sobre este procedimiento." (p.20)

6.2 Examen jurídico de licitud a los ataques informáticos dentro de una ciberguerra.

Una vez analizado como se realiza el examen jurídico a las armas o métodos nuevos, este debe ser aplicado en los ciberataques. El objetivo es saber si los ciberataques son lícitos o ilícitos dentro de un conflicto armado.

En un caso hipotético en que el Estado A decide utilizar el virus Stuxnet para atacar una central de energía ya que ha sido tomada por militares y esta se haya convertido en un objetivo militar, el Estado debería realizar según el artículo 36 del Protocolo Adicional I si este ataque informático es compatible con los fines del Derecho Internacional Humanitario puede ser usado pero, si este ataque va a generar perjuicios en la población civil y o bienes protegidos por el DIH no debe ser puesto en marcha.

- ✓ **Primer paso:** Determinar si los ataques informáticos dentro de la ciberguerra se encuentran regulados o no por un tratado o instrumento internacional.

Específicamente, la ciberguerra no se encuentra regulada ni analizada en ningún instrumento internacional.

- ✓ **Segundo paso:** Determinar si los ataques informáticos dentro de la ciberguerra respetarían las normas aplicables a todas las armas, medios y métodos de guerra.

Conforme el Articulo 35 del Protocolo adicional I, queda prohibido el empleo de métodos o medios de hacer la guerra que hayan sido concebidos para causar daños extensos, duraderos y al medio ambiente natural.

En el caso hipotético se menciona que el ataque informático se dirige a una planta de energía. La planta de energía consiste en transformar alguna clase de energía (química, cinética, térmica o lumínica, nuclear, solar entre otras), en energía eléctrica. Esto quiere decir que si el ataque se realiza a esta planta de energía las consecuencias serían para los combatientes y para las personas civiles, incluso los enfermos y los heridos correrían peligro por diferentes motivos.

Este ataque al afectar la central de energía estaría generando daños extensos, duraderos e incluso medio ambientales. Si bien es cierto no es necesario, para realizar un ataque informático, componentes químicos que generarían un gran impacto ambiental; empero para el caso hipotético esta situación se puede ver posterior al ataque realizado.

Por lo expresado este ataque no respetaría las normas aplicables a todas las armas, medios y métodos de combate.

- ✓ **Tercer paso: El ataque informático dentro de una ciberguerra debe estar conforme a los principios del Derecho Internacional Humanitario.**

El tema de los principios del Derecho Internacional Humanitario ya ha sido analizado en l Capítulo V del presente trabajo y se concluyó que algunos principios corren peligro de ser vulnerados por un ataque cibernético.

Al concluir este análisis identificamos que los ataques cibernéticos realizados dentro de un conflicto armado, según el artículo 36 del Protocolo adicional I, se considerarían armas ilícitas bajo las premisas del Derecho Internacional Humanitario.

CAPITULO VII

La Ciberseguridad en el Perú

La tecnología en todos los Estados ha ido avanzando y por ello es necesario que su normativa y sus instituciones se encuentren acorde a este avance No solo las Potencias deben tratar de resolver los problemas que actualmente se presenta con el avance de la tecnología. Si bien cierto, estos Estados, son los más propensos a recibir cualquier tipo de amenaza de parte de otro Estado, no son los únicos que los reciben.

Los países en constante crecimiento, son aquellos que se encuentran más vulnerables que otros, ya muchas veces su infraestructura y su normativa no se encuentra acorde a las necesidades y avances que se van encontrando.

Como anteriormente se ha dicho la ciberguerra es un reto, no solo para el Derecho Internacional sino también para la Comunidad Internacional. Para enfrentar una ciberguerra es necesario que todos los Estados nos encontremos

preparados; esto quiere decir que la infraestructura debe ser la adecuada, la organización Estatal debe ser idónea y la normativa debe estar acorde al Derecho Internacional Humanitario. Antes de empezar la redacción de este capítulo es importante resaltar que el Estado peruano, si bien es cierto, no se encuentra preparado completamente para afrontar una ciberguerra, este ya realizado sus primeros avances como lo veremos a continuación.

7.1 Los ataques informáticos en la normativa peruana

En el diario “La Primera Digital” (2014) se menciona que “El Perú ocupa el cuarto lugar en América en ataques informáticos.” En la actualidad la población peruana (instituciones estatales, privadas, personas naturales, entre otros) usa con mayor frecuencia las computadoras para almacenar información relevante, incluso esta información puede ser de interés nacional.

Es por ello que el Estado Peruano en el año 2003 creó la Oficina Nacional de Gobierno Electrónico e Informática (ONGEI). ONGEI, es el Órgano Técnico Especializado que depende del Despacho de la Presidencia de Consejo de Ministro (PCM), una de sus funciones principales está vinculada a la normatividad informática, la seguridad de la información, el desarrollo de proyectos emblemáticos en Tecnologías de la Información y la Comunicación (TIC), brindar asesoría técnica e informática a las entidades públicas, así como, ofrecer capacitación y difusión en temas de Gobierno Electrónico y la modernización y descentralización del Estado.

No solo tenemos la creación de este Órgano sino que también el Estado Peruano ha venido implementando una serie de normas e iniciativas presentadas por diferentes organismos públicos, orientadas a establecer una política de seguridad informática. Esto quiere decir que los ataques informáticos en el Perú

no pasan desapercibidos; actualmente contamos con una la Ley Nº 30096 – Ley de los delitos informáticos.

Según el ISSA (Information Systems Security Association) “El Perú es uno de los países que poco ha legislado en temas de seguridad de la información y seguridad informática y, sobretodo, en planeamiento de ciber defensa y ciber seguridad. No solamente hablamos de proteger una página web, sino estrategias de seguridad nacional.”

Entonces de todo ello se desprende que dentro del Estado Peruano, algunos ataques cibernéticos son regulados por el derecho penal. Ello nos confirma que actualmente en el Perú no existe un Plan Estratégico de Ciberseguridad.

7.2 Desarrollo de un Plan Estratégico de Ciberseguridad en Perú

Es necesario desarrollar un Plan Estratégico de Ciberseguridad en el Perú, ya que los ataques cibernéticos todos los días nos enfrentan. El cibercrimen, la ciberdelincuencia, el ciberdelito son temas que actualmente están en pleno desarrollo.

El ISSA presentó un proyecto denominado “Propuesta Política de Estrategia Nacional de Ciberseguridad” dentro de esta propuesta el ISSA busca la relación entre la ciberseguridad y la seguridad nacional y menciona así que : “La Seguridad Nacional se desarrolla dentro del ámbito del Ciberespacio para la protección de las infraestructuras críticas, territorio, organizaciones públicas y privadas y los ciudadanos, en términos de asegurar el funcionamiento de las infraestructuras públicas y privadas, que representan centros de gravedad dentro del funcionamiento del estado y cuya neutralización ocasionaría suspender servicios esenciales. La vigilancia y protección del territorio nacional involucra el

empleo intensivo de Tecnología de Información y Comunicaciones, el desarrollo de proyectos como el Sistema de Vigilancia Amazónicos y Nacional (SIVAN), se constituye como el gran centro proveedor de información para todas las agencias del estado y para el sector privado así como centros de investigaciones científica, su protección se enmarca dentro de los alcances de esta política dado que representa una plataforma para el desarrollo. El desarrollo de iniciativas como el PIDE, la implementación de la Agenda Digital 2.0. Gobierno Electrónico y Gobierno Abierto, representa desafíos para el estado en términos de garantizar la seguridad dado que se sostienen en Tecnologías de Información y Comunicaciones, por lo que el desarrollo de la capacidad de Ciberdefensa representan un asunto de carácter estratégico para el país." (p. 23)

La estrategia propuesta por el ISSA busca fortalecer las capacidades del Estado y mejorar las defensa para cualquier ataque cibernético. Estos ataques se pueden desarrollar de manera continua (como los ataques de robo de la información, espionaje que recibimos a diario) o dentro de un conflicto armado.

7.3 La creación del Comité Especializado en Ciberguerra dentro del Ministerio de Defensa del Perú.

La implementación del Derecho Internacional Humanitario en el Perú tiene que seguir evolucionando. Las nuevas armas que son identificadas y estudiadas por otros países, también deben de ser analizadas en el Perú. Muy aparte del "Plan Estratégico de la ciberguerra" es necesario la creación de un órgano que se encargue de este tema; por ello se plantea la creación de un Comité Especializado en Ciberguerra.

Este Comité debe ser multidisciplinario, ya que es necesaria la intervención de diferentes especialidades; la experiencia militar, jurídica, informática y ambiental

hará que sus funciones sean desarrolladas de manera más eficiente. Las funciones que resaltan de este Comité son: planear, coordinar, ejecutar y conducir operaciones cibernéticas (activas y/o pasivas); la función más importante que tendría es la prevención de ciberataques dentro de un conflicto armado para poder garantizar los principios del Derecho Internacional Humanitario. Con el control que este Comité ejercería sobre parte del ciberespacio lograría limitar los efectos colaterales que pueden ocasionarse en caso de ser víctimas de un ciberataque dentro de un conflicto armado.

Este Comité debería de formar parte del Departamento de Seguridad Nacional "integrar a todas las agencias del Estado, lideradas por la Coordinadora de Respuestas ante incidentes Teleinformáticas de la Administración Publica (Pe-CERT), que articule a los elementos operativos del Ministerio de Defensa y del Ministerio de Interior en el ciberespacio, cibercomando, DIVINDAT, los que a través de una comisión multisectorial se integraran con las Universidades, colegios profesionales, la Comunidad a proteger, tanto pública como privada." (ISSA, 2012, p.26)

A la falta de una normativa internacional sobre "los ciberataques dentro de un conflicto armado" cada Estado debe realizar un análisis para saber si determinada arma es compatible o no con el Derecho Internacional Humanitario. Pues bien, este Comité debe de encargarse de realizar un Informe público en el cual el Estado Peruano emite su opinión acerca de la licitud de los ciberataques dentro de un conflicto armado, para que este pueda ser contrastado con otros informes de diferentes Estados y así promover la creación de instrumento internacional que regula los ciberataques.

Por último, es importante mencionar que este Comité encargará de trabajar los ataques cibernéticos dentro de un conflicto armado y apoyar a las instituciones como al PCM en la cual existe la Oficina Nacional de Gobierno Electrónico e Informática, a la Coordinadora de Respuestas a Emergencias en Redes Teleinformáticas de la Administración Publica del Perú y finalmente al Comando Conjunto de las Fuerzas Armadas que se encuentra en la Octava División de Estado Mayor Conjunto que es la División de Operaciones de Información (dentro de esta oficina se encuentra el Departamento de ciberdefensa).

CAPITULO VIII

Discusión y Resultados

A continuación se presentan los resultados de la investigación en base a la información recogida mediante las técnicas e instrumentos presentados en el proyecto de investigación. Estos resultado se objetivizan mediante cuadros estadísticos y entrevistas de acuerdo a las hipótesis del trabajo y su relación con cada una de las variables.

Encuesta a 50 estudiantes de derecho.

1.- Nivel de conocimiento de las nuevas armas que se utilizan en los conflictos armados.

GENERO DE LA PERSONA	SI	NO
Masculino	14	14
Femenino	15	07
RESULTADO	**29**	**21**

***** (29) Estudiantes conocen sobre las nuevas armas que se utilizan en los conflictos armados.

2.- Conocimiento sobre la ciberguerra.

GENERO DE LA PERSONA	SI	NO
Masculino	18	10
Femenino	19	03
RESULTADO	**37**	**13**

***** (37) Estudiantes tienen conocimiento de una ciberguerra.

3.- Los principios del Derecho Internacional humanitario vulneran la ciberguerra.

GENERO DE LA PERSONA	SI	NO
Masculino	15	13
Femenino	19	03
RESULTADO	**34**	**16**

*(34) Estudiantes opinan que la ciberguerra vulnera los principios del Derecho Internacional Humanitario.

4.- El ciberespacio un nuevo escenario de guerra.

GENERO DE LA PERSONA	SI	NO
Masculino	23	5
Femenino	19	03
RESULTADO	**42**	**08**

* (42) Estudiantes opinan que ciberespacio es un nuevo escenario para la guerra.

5.- Países que se encuentran preparados para una ciberguerra.

- ✓ Dentro de los países mencionados en la encuesta se encuentran: Estados Unidos, Rusia, Brasil, Alemania, Países de Europa, Japón, China, Francia e Inglaterra

6.- Perú se encuentra o no preparados para enfrentar una ciberguerra.

GENERO DE LA PERSONA	SI	NO
Masculino	01	27
Femenino	02	20
RESULTADO	**03**	**47**

* (47) Estudiantes opinan que el Perú no se encuentra preparado para enfrentar una ciberguerra.

7.- Plan Estratégico de ciberseguridad en el Perú.

GENERO DE LA PERSONA	SI	NO
Masculino	24	04
Femenino	17	05
RESULTADO	**41**	**09**

* (41) Estudiantes opinan que es necesario la creación de un Plan Estratégico de ciberseguridad en el Perú.

8.- Creación de una Departamento Especializado para la ciberguerra.

GENERO DE LA PERSONA	SI	NO
Masculino	20	08
Femenino	13	9
RESULTADO	**33**	**17**

* (33) Estudiantes aceptan la creación de un Departamento Especializado para la Ciberguerra.

9.- Capacitación del personal de las fuerzas armadas para enfrentar una ciberguerra.

GENERO DE LA PERSONA	SI	NO
Masculino	22	06
Femenino	21	01
RESULTADO	43	07

* (43) Estudiantes opinan que el personal de las fuerzas armadas deben de ser capacitados para enfrentar una ciberguerra.

10.- ¿Perú ha logrado implementar y difundir el Derecho Internacional Humanitario?

GENERO DE LA PERSONA	SI	NO
Masculino	02	26
Femenino	03	19
RESULTADO	05	45

* (45) Estudiantes llegaron a la conclusión de que no se ha logrado difundir e implementar el Derecho Internacional Humanitario. (Tabla de mi autoría)

Todos estos datos confirman, de manera empírica, la necesidad de crear un Comité Especializado en Ciberguerra, difundir e implementar de manera más continúa la normativa del Derecho Internacional Humanitario y sobre todo estas encuestas resaltan la necesidad de crear un Plan Estratégico de Ciberseguridad en el Perú.

CAPITULO IX

Conclusiones y Recomendaciones

9.1 Conclusiones

a) Los ataques informáticos son regulados a nivel interno siempre y cuando no se desarrollen dentro de un conflicto armado. En el caso de que los ciberataques se realicen dentro de un contexto armado, estos son regulados por el Derecho internacional Humanitario denominándose “ciberguerra”.

b) Los ataques dentro de la ciberguerra deben ser dirigidos a la infraestructura estatal y debe generar un daño determinable.

c) Los principios del Derecho Internacional Humanitario o Derecho Internacional de los Conflictos Armados muchas veces son vulnerados por los ciberataques, ya que sus efectos pueden ocasionar daños colaterales y males superfluos. Incluso el principio de protección

ambiental también se puede ver vulnerado cuando este afecte bienes naturales necesarios para la supervivencia de la población civil. Esta conclusión responde nuestro problema principal de manera afirmativa.

d) Al no existir normativa internacional que regule específicamente los ataques cibernéticos dentro de un conflicto armado, es necesario que cada uno de los Estados realicen un análisis jurídico para determinar la licitud o ilicitud de los ataques cibernéticos: esto es conforme al artículo 36 del Protocolo Adicional I.

e) En el Perú, la normativa cibernética se encuentra en constante evolución. Actualmente no se cuenta con una Oficina Especializada para la Ciberguerra; por ende, es importante del Comité Especializado en Ciberguerra para que este planee, organice, ejecute, coordine y conduzca operaciones cibernéticas activas y pasivas.

Con todas las conclusiones antes mencionadas se confirma la afirmación de cada una de nuestras hipótesis, sobre todo la hipótesis del problema principal.

9.2 **Recomendaciones**

a) A nivel Internacional

- ✓ Los Estados deben de realizar el análisis establecido en el artículo 36 del Protocolo Adicional I de los Convenios de Ginebra para así determinar la licitud o ilicitud de los ataques informáticos.

  Los análisis que realiza cada Estado deben ser publicados y accesibles para que otros Estados tomen conocimiento y emitan sus informes

respectivos. Esto logrará que los Estados se den cuenta de manera a más rápida la necesidad de regular ciertas materias.

- ✓ El Comité Internacional de la Cruz Roja en la próxima Conferencia Internacional de la Cruz Roja y de la Media Luna Roja debe proponer la elaboración de un tratado sobre ataques cibernéticos dentro de los conflictos armados ya que no es suficiente lo establecido por los Convenios de Ginebra y sus Protocolos Adicionales.

b) A nivel Nacional

- ✓ Es necesaria la elaboración de un Plan Estratégico de ciberseguridad para el Perú.

- ✓ Es importante de igual manera la creación de un Comité Especializado en Ciberguerra dentro del Ministerio de Defensa para poder garantizar la normativa del Derecho Internacional Humanitario.

- ✓ El Estado Peruano debe difundir con más precisión el Derecho Internacional Humanitario para que las personas conozcan y aporte más a nuestra cultura jurídica.

CAPITULO X

Fuentes de información

10.1 Referencias Bibliográficas

10.1.1 Libros:

- Gómez, A. (2012) *El ciberespacio como escenario del conflicto. Identificación de las amenazas.* En J.R. Casa (Ed.), El Ciberespacio. Nuevo escenario de confrontación (pp. 170-203). España: Ministerio de Defensa.
- Novak, F. & otros (2003) *Derecho Internacional Humanitario.* Lima: Instituto de Estudios Internacionales de la Pontificia Universidad Católica del Perú.
- Salmòn E. (2004) *Introducción al Derecho Internacional Humanitario.* Lima: Instituto de Democracia y Derechos Humanos de la Pontificia Universidad Católica del Perú.

- Valencia A. (2013) *Derecho Internacional Humanitario: Concepto básicos – Infracciones en el conflicto armado colombiano.* Bogotá: Oficina del alto comisionado de las Naciones Unidas – Derechos Humanos y ACDI – Canadá.
- Henckaerts, J-M & B. (2007) El Derecho Internacional Humanitario Consuetudinario. (Vol. I) (M. Serrano Garcìa. Trad.) Buenos Aires, Argentina: Comité Internacional de la Cruz Roja.
- Gonzales, J. G. (1988). El concepto de soberania en la historia constitucional. En B. Bernal, *Memoria del IV Congreso de Historia del Derecho Mexicano* (pág. 573). Mexico D.F.: Universidad Nacional Autonoma de Mexico.
- Lawand, K. (2006) *Guia para el examen jurìdico de las armas, los medios y los mètodos de guerra nuevos*. Ginebra: Comité Internacional de la Cruz Roja.
- Pictect , J., Casser , H.-P., Junod, S.-S., Pilloud, C., De Preux, J., Sandoz, Y., . . . Zimmermann, B. (2001). *Comentario del Protocolo del 8 de junio de 1977 adicional a los Convenios de Ginebra del 12 de agosto 1949 relativo a la protecciòn de las victimas de los conflictos armados internacionales. (Protocolo I).* Colombia: Plaza & Janes Editores.
- Ulloa, A. (1957). *Derecho Internacional Público .* Madrid: Ediciones Iberoamericanas, S.A.
- Monroy, G. (2011). *Derecho Internacional Público*. Bogotá: Editorial Temis S.A. pp. 812.

- Swinarski, Ch. (1984). *Introducción al Derecho Internacional Humanitario*. San José/ Ginebra: Comité Internacional de la Cruz Roja/ Instituto Interamericano de Derechos Humanos. pp. 72
- Jaramillo D. (1975). *Derecho Internacional humanitario*. Bogotá, Universidad Santo Tomás, pp.159.
- Roda, J.M. (1979). *Derecho Internacional Público.* Buenos Aires: Editora Argentina. pp. 3.
- De Mullinen F. (2005). *Manual sobre el derecho de la guerra para las fuerzas armadas.* Ginebra, Suiza: Comité Internacional de la Cruz Roja.
- Ossorio, A. (2002). *Planeamiento Estratégico*. Buenos Aires, Argentina: Instituto Nacional de la Administración Pública.

10.1.2 Investigaciones y/o casos

- Schmitt, M. (2013). *The Tallinn Manual on the International Law Applicable to CyberWarfare.* [El Manual de Tallinn en el Derecho Internacional aplicable a la ciberguerra.] New York: Cambridge University.
- Opinión Consultiva de la Corte Internacional de Justicia sobre la legalidad de la amenaza o el empleo de armas nucleares. A/51/218. (Corte Internacional de Justicia) p.2
- Resolución Nº 2675 (XXV). Principios básicos para la protección de las poblaciones civiles en los conflictos armados. Publicado en la página oficial de las Naciones Unidas, el 9 de diciembre de 1970.
- Revilla, P. (2006) *La función de mantenimiento de la paz en la Carta de las Naciones Unidas: propuesta de regulación de la intervención humanitaria como operación de mantenimiento de la paz.* (Tesis para

optar el Título Profesional de Abogado). Universidad Nacional Mayor de San Marcos, Lima.

10.2 Referencia Hemerogràficas

- Comité Internacional de la Cruz Roja, (2011, Noviembre, 28) XXVIII Conferencia Internacional de la Cruz Roja y de la Media Luna Roja, diciembre de 2003, “El derecho internacional humanitario y los retos de los conflictos armados contemporáneos. Informe preparado por el Comité Internacional de la Cruz Roja”, septiembre de 2003.
- Diallo,Y., (1978). Tradición, África y Derecho Humanitario. Ginebra: Comité Internacional de la Cruz Roja, pp. 3-4.
- Schmitt, M. (2002) La guerra de la información: los ataques por vía informática y el jus in bello. Revista Internacional de la Cruz Roja. Nº 846, p. 365 – 399.
- Dosvvald-Beck, L. (1997). El Derecho internacional humanitario y la Opinión consultiva de la Corte Internacional de Justicia sobre la licitud de la amenaza o del empleo de armas nucleares. *Revista Internacional de la Cruz Roja, 139,* 37-58.
- Ortega, M. (1990). La funció Jurisdiccional del Estado. *Revista de la Facultad de Derecho de Mexico*, 128 - 165.
- Penna, L. (1989). Disposiciones escritas y consuetudinarias relativas a la conducciòn de hostilidades y trato que recibian las victimas de conflictos armados en la antigua India. *Revista Internacional de la Cruz Roja* , 352-368.
- Boothby, W. (2012). Some legal challenges posed by remote atack. *International Review of the Red Cross*, 876.

10.3 Referencias electrónicas

- IEE Spectrum (2013). *The real story of Stuxnet.* Recuperado de http://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet el 14 de Noviembre de 14.
- Pictect, J. (1986) *Desarrollo y Principios del Derecho Internacional Humanitario.* Recuperado el 16 de enero de 2015 de https://www.icrc.org/spa/resources/documents/misc/desarrollo_y_principios.htm
- El Mundo (2012), *Descubren Flame, un virus especializado en "ciberespionaje".* Recuperado de http://www.elmundo.es/elmundo/2012/05/28/navegante/1338218199.html el 14 de Noviembre de 2014.
- San Agustín. *La Ciudad de Dios*. Buenos Aires: Poblet, 1945, cap. XIX (15).
- Aguirre G. (2007). *Qué es el ciberespacio?*. Recuperado de: http://aguirregimena-imdtp1.blogspot.com/2007/09/que-es-un-ciberespacio.html, el 09 de Octubre de 2014.
- Gomez-Robledo, A. (1993). *Jurisdicción interna, Principio de No Intervención y derecho de injerencia humanitaria.* Boletín Mexicano de Derecho Comparado, N° 76, 79 – 97. Recuperado de http://biblio.juridicas.unam.mx/revista/pdf/DerechoComparado/76/art/art3.pdf
- Alba, M. (2013). *Derecho Internacional carece de legislación contra espionaje.* Recuperado el 1 de abril de 2015 de

http://www.eluniversal.com/internacional/131026/derecho-internacional-carece-de-legislacion-contra-espionaje

- Ticehurst, R. (1997). *La cláusula de Martens y el derecho de los conflictos armados.* Revista Internacional de la Cruz Roja. Recuperado el 3 de enero de 2015 de https://www.icrc.org/spa/resources/documents/misc/5tdlcy.htm
- Dunant, H. (1982). *Recuerdo Solferino*. Ginebra: Comité Internacional de la Cruz Roja. Recuperado el 12 de febrero del 2014 de https://www.icrc.org/spa/assets/files/other/icrc_003_p0361.pdf
- Peña, L. (1986). *Desarrollo y principios del Derecho Internacional Humanitario.* Recuperado el 16 de enero de 2015 de https://www.icrc.org/spa/resources/documents/misc/desarrollo_y_principios.htm
- Rodriguez—Villasante y Prieto, J.L. (2009) La protección del personal humanitario por el Derecho Internacional Humanitario en los conflictos armados internacionales. Recuperado de *http://www.cruzroja.es/dih/pdfs/temas/1_6/1_6.pdf* el 19 de julio de 2014.
- Stefan, K. (02 de 04 de 2015). *El ejercicio de la soberanía de los Estados.* . Obtenido de Biblioteca Juridica Virtual del Instituto de Investigaciones Jurídicas de la UNAM: http://biblio.juridicas.unam.mx/libros/6/2790/6.pdf
- *Stuxnet: El virus capaz de crear "el caos absoluto"* (n.d.) Recuperado de http://actualidad.rt.com/actualidad/view/111953-stuxnet-virus-iran, el 14 de Octubre de 2014

- Valenzuela, J. (2012) *Virus Flame: la primera bomba atómica de la ciberguerra.* Recuperado de http://blogs.elpais.com/cronica-negra/2012/06/virus-flame-la-primera-bomba-atomica-de-la-ciberguerra.html el 14 de Noviembre de 2014.
- Comité Internacional de la Cruz Roja (2008) *¿Cuál es la definición de "conflicto armado" según el derecho internacional humanitario?* Recuperado de https://www.icrc.org/spa/assets/files/other/opinion-paper-armed-conflict-es.pdf el 20 de Julio de 2015.

ANEXOS

ANEXOS 1

Propuesta “Plan Estratégico de ciberseguridad en el Perú”

I. PRESENTACION

El Perú es un Estado propenso a diversos ataques, ya que su historia se fundamenta en diversas guerras. Estos ataques se han ido desarrollando conforme la evolución del ser humano y cada día se ha sofisticado.

La tecnología es la ayuda más cercana que tiene el hombre para poder realizar sus labores cotidianas, laborales y/o estudiantiles. El internet se ha convertido en parte indispensable de sus vidas y esto se refleja en diversas estadísticas realizadas por los medios de comunicación.

Así como la tecnología puede ser de mucha ayuda, en ocasiones esta se convierte en nuestro enemigo incógnito e indestructible. El internet ya no es usado para satisfacer a los usuarios en sus conocimientos, sino que este, es usado para destruir y/o amenazar infraestructuras privadas o públicas, alterar información de las entidades privadas o públicas; alterar, sustraer, modificar o eliminar información relevante de los usuarios, entre otros.

Es por ello que los Estados y, sobre todo el peruano, deben de contar con un “Plan estratégico de ciberseguridad” para poder prevenir, afrontar y reducir los ataques cibernéticos en diversas ocasiones.

La presente propuesta abordará los objetivos a lograrse, la estrategia a ser utilizada y propondrá la creación de un Departamento Especializado en Ciberguerra el cual se ubicará dentro del Ministerio de Defensa.

II. CONCEPTO

La Estrategia de Ciberseguridad Nacional es el documento estratégico que sirve como fundamento al Estado Peruano para desarrollar las previsiones de la Estrategia de Seguridad Nacional en materia de protección del ciberespacio con el fin de implantar de forma coherente y estructurada acciones de prevención, defensa, detección y respuesta frente a las ciberamenazas. (Gobierno de España, 2013, p. 3)

III. MISION

Proteger a la infraestructura nacional y privada, la información de los ciudadanos de los ataques cibernéticos y mantener estabilizadas nuestras fuentes de información.

Fijar directrices del uso seguro del ciberespacio para los ciudadanos y para las organizaciones privadas en cooperación con todas las Administraciones Públicas.

IV. VISION

El Plan Estratégico de ciberseguridad activo dará inicio a diferentes Unidades dentro del Ministerio de Defensa, los cuales deberán salvaguardar la información cibernética de los diferentes usuarios (empresas privadas, organismos estatales y ciudadanos) y prevenir cualquier daño para el Estado peruano originado por un ciberataque.

V. ANALISIS DE LA SITUACION ACTUAL

El Perú no cuenta con un “Plan Estratégico de ciberseguridad” dado que las autoridades nacionales no han logrado implantar la tecnología en todas sus áreas. Es así que el Perú necesita, antes que nada capacitar a sus funcionarios y/o servidores públicos para que puedan familiarizarse y afrontar los nuevos retos del ciberespacio.

Con respecto a la legislación, contamos con un avance en algunos temas informáticos; se ha creado la Oficina Nacional de Gobierno Electrónico e Informática (ONGEI), se ha creado la ley penal de delitos informáticos “- Ley Nº 30096” y el ISSA en el año 2012 presentó un proyecto denominado “Propuesta Política de Estrategia Nacional de Ciberseguridad” el cual iba a ser evaluado para su aprobación.

VI. PRINCIPIOS

Coordinación de esfuerzos

Todas las entidades (públicas y privadas) deberán colaborar de manera directa con el Ministerio de Defensa para poder hegemonizar nuestra defensa cibernética.

Responsabilidad compartida

Todos los ciudadanos, organismos públicos y organizaciones privadas deben de sentirse comprometidos e implicados con ciberseguridad. Ello coadyuvará a mejorar anualmente nuestro sistema de defensa cibernético.

Cooperación Internacional

El Estado Peruano fomentará y asistirá a las eventos internacionales para sobre seguridad nacional o ciberseguridad buscando fortalecer y/o mejorar nuestra estrategia de ciberseguridad.

VII. OBJETIVOS

Los objetivos de la propuesta del “Plan Nacional Estratégico de Ciberseguridad en el Perú” son los siguientes:

- **Objetivo Principal**

Proteger las infraestructuras de los organismos estatales, las fuerzas armadas y a los ciudadanos pertenecientes al territorio peruano que sean objetos de ataques cibernéticos nacionales o internacionales.

- **Objetivos Secundarios**

Potenciar las capacidades de prevención, reacción, análisis, recuperación y coordinación frente a los ataques cibernéticos.

Asegurar la implementación de normativa adecuada para salvaguardar nuestra seguridad cibernética.

Mejorar las capacidades de defensa que tiene el Estado peruano respecto a un ciberataques que se realizan de manera cotidiana.

Estudiar e implementar el sistema de defensa cibernético a utilizar, en caso de un conflicto armado internacional.

Salvaguardar la normativa interna e internacional conforme al derecho vigente.

Fortalecer la cooperación judicial y policial a nivel nacional e internacional.

Contribuir a la mejora de la ciberseguridad a nivel internacional.

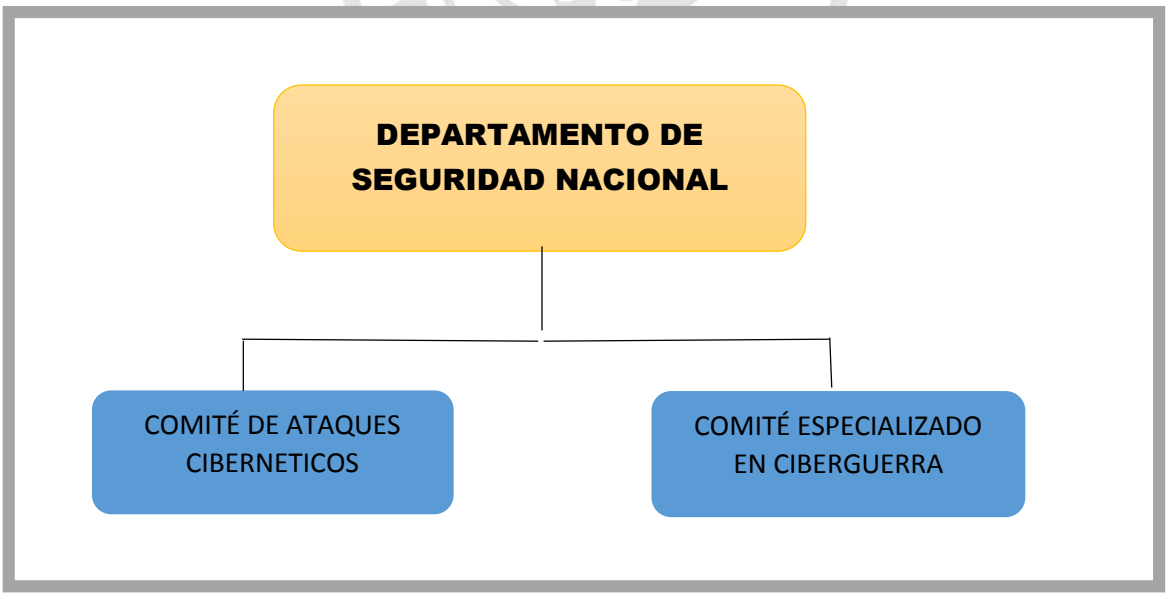
VIII. ESTRATEGIA

La misión y visión del presente “Plan de ciberseguridad nacional del Perú” se fundamenta en sus principios y objetivos plasmados. Para lograr con el objetivo principal es necesario contar con una estructura orgánica precisa a estos efectos, la cual se detallara a continuación y se encontrará al mando del Ministerio de Defensa.

A. Departamento de Seguridad Nacional

B. Comité Especializado en Ataques informáticos

C. Comité Especializado en Ciberguerra



IX. ESTRUCTURA DEL DEPARTAMENTO DE SEGURIDAD NACIONAL

- **Departamento de seguridad nacional**

  El Departamento de Seguridad Nacional dependerá directamente del despacho del Ministerio de Defensa y trabajará en coordinación con el Comando Conjunto de las Fuerzas Armadas.

  Adecuará la infraestructura estatal a una moderna y adquirirá equipos con tecnología necesarios para las entidades estatales.

- **Comité de ataques cibernéticos**

  El Comité brindará apoyo y asesoría al Departamento de Seguridad Nacional para lograr los objetivos de la Estrategia Nacional en Ciberseguridad respecto a lo ciberataques.

  Asimismo se encargará de organizar, designar y crear oficinas con sus funciones para salvaguardar la información y la infraestructura Estatal, Privada y de los ciudadanos.

  Verificar que en las instituciones públicas y privadas ingresen de manera sencilla y fácil toda la documentación que se requiera.

- **Comité especializado en ciberguerra**

  El comité brindará apoyo y asesoría al Departamento de Seguridad Nacional en materia de conflictos armados cibernéticos.

  Prevendrá y afrontará, con el Comando Conjunto de las Fuerzas Armadas, conflictos armados cibernéticos siempre con la dirección del Departamento de Seguridad Nacional y la aprobación del Ministerio de Defensa.

  Propondrán proyectos normativos para consulta ante el Ministerio de Defensa y lograr la aprobación ante el Congreso de la República en materia de conflictos armados cibernéticos.

  Garantizarán el respeto de los principios del Derecho Internacional Humanitario, adecuando la normativa existente.

  Acudirán a los eventos internacionales sobre la ciberseguridad dentro de un conflicto armado.

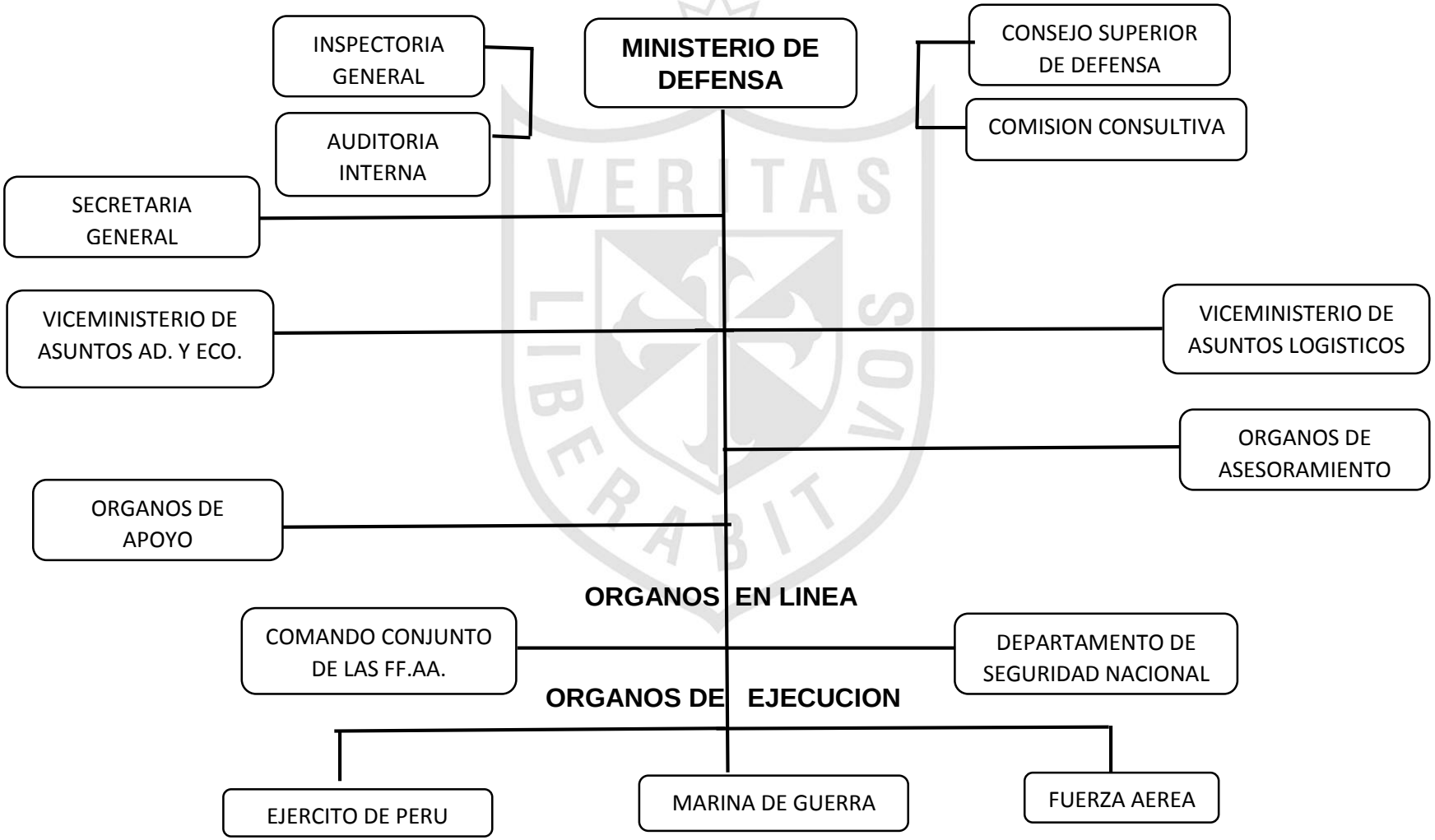
  Elaborarán un plan estratégico de ciberdefensa para enfrentar los ataques cibernéticos y una próxima ciberguerra.

X. FUNDAMENTO LEGAL

La presente Estrategia Nacional de Ciberseguridad en el Perú se presenta en base a la Constitución Política del Perú y respetando y aplicando los principios del Derecho Internacional Humanitario y la Carta de Naciones Unidas la cual tiene como objetivo final salvaguardar la paz y seguridad internacional.

ANEXO 2

Proyecto de Organigrama del Ministerio de Defensa



ANEXO 3

Conceptos básicos

a) Ataques informáticos

Según Schmitt (2002) “Los ataques a través de redes informáticas (ARI), que pueden considerarse como guerra de la información o como simples operaciones de información, son acciones destinadas a “perturbar, rechazar, deteriorar o destruir la información contenida en ordenadores o en redes informáticos, o los propios ordenadores y redes informáticas.”

b) Ciberguerra

Laurent Gisel (2013) señala que “Cuando hablamos de guerra cibernética, nos referimos solamente a los medios bélicos que consisten en operaciones cibernéticas que alcanzan el nivel de un conflicto armado o son conducidas en el contexto de un conflicto armado, según los términos del Derecho Internacional Humanitario.”

c) Ciberespacio

La Publicaciòn Conjunta 1-02 del Departamento de Defensa de los Estados Unidos lo define como: “ un dominio global dentro del entorno de la información, compuesto por una infraestructura de redes de tecnologías de información interdependientes, que incluye internet, las redes de telecomunicaciones, los sistemas de información y los controladores y procesadores integrados junto con sus usuarios y operadores.” (Gomez, A. 2012, pp. 170-171)

d) Ciberseguridad

Es la seguridad que debe existir en el ciberespacio.

e) Combatiente:

Según Schmitt (2002) “Un combatiente es un miembro de las fuerzas armadas que no forman parte del personal médico ni religioso. Las fuerzas armadas “se componen de todas las fuerzas, grupos y unidades armados y organizados, colocados bajo un mando responsable de la conducta de sus subordinados ante (una) parte … (d) deberán estar sometidas a un régimen de disciplina interna que haga cumplir, inter alias, las normas de derecho internacional aplicables en los conflictos armados”.

Así mismo, “Combatiente” es todo miembro de las fuerzas armadas, excepto el personal sanitario y religioso. Cuando participen en una acción militar preparatoria, los combatientes deben distinguirse de la población civil. (De Mulinen, F., 1991, p. 12)

f) Conflicto armado:

Según el artículo 2 común a los Convenios de Ginebra de 1949 un conflicto armado internacional es aquel en que se enfrentan “Altas Partes Contratantes”, en el sentido de Estados. Un conflicto armado internacional ocurre cuando uno o más Estados recurren a la fuerza armada contra otro Estado, sin tener en cuenta las razones o la intensidad del enfrentamiento. Las normas pertinentes del DIH pueden ser aplicables incluso si no hay hostilidades abiertas. Además, no hace falta que se haga oficialmente una declaración de guerra o un reconocimiento de la situación.

Como jurisprudencia podemos mencionar lo siguiente:

"… existe un conflicto armado siempre que se recurra a la fuerza armada entre los Estados o violencia armada prolongada entre las autoridades gubernamentales y grupos armados organizados, o entre tales grupos de un Estado. El derecho internacional humanitario se aplica desde el inicio de tales conflictos armados y se extiende más allá de la cesación de hostilidades hasta que se celebra un tratado de paz; o en, el caso de conflictos internos, se alcanza un acuerdo pacífico. Hasta ese momento, el derecho internacional humanitario continúa aplicándose en el territorio entero de los Estados en guerra o, en caso de conflictos internos, todo el territorio bajo control de una parte, si ahí toma lugar o no un combate real. (Tribunal Penal Internacional de la antigua Yugoslavia, caso Tadic, decisión del 2 de octubre de 1995, segunda instancia, párr.. 70. Traducción no oficial de Rafael Prieto Sanjuán, *Tadic*; *internacionalización de conflictos internos y responsabilidad individual*, Pontificia Universidad Javeriana, Biblioteca Jurídica Diké, Bogotá, 2005, p.126.)

Schmitt (2002), menciona que en los comentarios de los Convenios de Ginebra de 1949 y de los Protocolos adicionales de 1977, publicados por el Comité Internacional de la Cruz Roja, se adopta un punto de vista muy amplio acerca del significado de este término. En los primero se define un conflicto armado como "toda diferencia que surja entre dos Estados y que dé lugar a la intervención de fuerzas armadas …, incluso si una de las partes niega la existencia de un estado de guerra y sin importar la duración o el carácter más o menos mortífero del conflicto".

No solo la jurisprudencia se ha encargado de establecer qué es un conflicto armado tanto internacional como no internacional, sino también la doctrina lo desarrolla. Según D. Schindler,"es posible dar por sentado que hay un conflicto armado en el sentido del artículo 2 común a los Convenios de Ginebra cuando partes de las fuerzas armadas de dos Estados se enfrentan entre ellas (…) Cualquier tipo de utilización de las armas entre dos Estados hace que los Convenios surtan efecto.

El Stockholm International Peace Research Institute (Sipri) en sus Yearbooks de 1989 y 1990, señalan que un conflicto armado importante es "un combate prolongado entre las fuerzas militares de dos o más gobiernos, o de un gobierno y movimientos de resistencia organizados, utilizando armas fabricadas y en el que el número de muertos resultantes de los enfrentamientos es de mil personas como mínimo.

g) Espionaje

La definición auténtica del concepto de espía en el Derecho de la Guerra hay pues que buscarla en el art. 29 del Reglamento de la Guerra Terrestre, anexo al Convenio II de la Haya de 1899: "No se puede considerar como espía más que al individuo que obrando clandestinamente o con pretextos falsos, recoge o trata de recoger informes en la zona de operaciones de un beligerante con la intención de comunicarlos a la parte contraria"

Valladares, G. (2003) manifiesta que:

"El artículo 46 del Protocolo I regula el espionaje circunscribiéndolo exclusivamente al miembro de las fuerzas armadas y así en sus apartados 2 y 3 dice que se considerará que realiza actividades de espionaje el miembro de las fuerzas armadas de una Parte en conflicto que, a favor de esa Parte, recoja o intente recoger información dentro de un territorio controlado por una Parte adversa siempre que, al hacerlo, vista el uniforme de las fuerzas armadas a que pertenezca; o que siendo residente en territorio ocupado por una Parte adversa recoja o intente recoger información de interés militar dentro de este territorio, salvo que lo haga mediante pretextos falsos o proceda de modo deliberadamente clandestino."

h) Flame

Es un virus informático que afecta a diferentes ordenadores; muy poderoso y complejo, difícil de destruir.

i) Plan estratégico de ciberseguridad

Segùn Ossorio A. (2002) "El termino plan proviene del latín y significa "espacio que ocupa la base de un edificio" y más tarde se entendido como "diseño de un edificio" o más precisamente, "distribución del espacio que ocupa la base de un edificio". Lo que podría equivaler a "esquema básico de diseño de cimientos y base de un edificio.

El término "estrategia" en su raíz etimológica, designa originalmente al nombre del "puesto" del titular del ejército, el lugar de mayor jerarquía." (p. 12)

Con el correr del tiempo, se le denomina estrategia a aquellos conocimientos que se necesitan para lograr realizar determinada cosa.

El Plan estratégico quiere decir aquel documento en el cual se construye un determinado proyecto con los mejores conocimientos a aplicar.

j) Stuxnet

Es un gusano informático que apunta a los sistemas industriales de control que utilizan para controlar instalaciones industriales como plantas de energía eléctrica, represas, sistemas de procesamiento de desechos entre otras operaciones industriales.