UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE DERECHO

ELEMENTOS PARA EL DESARROLLO DE UNA CONVENCIÓN INTERNACIONAL EN MATERIA DE GUERRA CIBERNÉTICA.

T E S I S
QUE PARA OBTENER EL TITULO DE.
LICENCIADO EN DERECHO
PRESENTA:
HÉCTOR MANUEL MÁRQUEZ RIVERA

ASESORA
LIC. GRACIELA A. OSORIO VILLASEÑOR

MÉXICO, D.F. **2011**

VNIVERSIDAD NACIONAL
AVÍNOMA DE
MEXICO

FACULTAD DE DERECHO
SEMINARIO DE DERECHO INTERNACIONAL

DR. ISIDRO ÁVILA MARTÍNEZ
DIRECCIÓN GENERAL DE LA
ADMINISTRACIÓN ESCOLAR
PRESENTE

El alumno **HÉCTOR MANUEL MÁRQUEZ RIVERA** con número de cuenta **403086674** inscrita en el Seminario de Derecho Internacional bajo mi dirección, elaboró su tesis profesional titulada **"ELEMENTOS PARA EL DESARROLLO DE UNA CONVENCIÓN INTERNACIONAL EN MATERIA DE GUERRA CIBERNETICA"**, dirigida por la Maestra GRACIELA AMALIA OSORIO VILLASEÑOR, investigación que, una vez revisada por quien suscribe, se aprobó por cumplir con los requisitos reglamentarios, en la inteligencia de que el contenido y las ideas expuestas en la investigación, así como su defensa en el examen oral, son de la absoluta responsabilidad de su autor, esto con fundamento en el artículo 21 del Reglamento General de Exámenes y la fracción II del artículo 2º de la Ley Orgánica de la Universidad Nacional Autónoma de México.

De acuerdo con lo anterior y con fundamento en los artículos 18, 19, 20 y 28 del vigente Reglamento General de Exámenes Profesionales, solicito de usted ordene la realización de los trámites tendientes a la celebración del examen profesional del alumno mencionado.

El interesado deberá iniciar el trámite para su titulación dentro de los seis meses siguientes, contados de día a día, a partir de aquél en que le sea entregado el presente oficio, con la aclaración de que, transcurrido dicho plazo sin haber llevado a efecto el examen, caducará la autorización que ahora se le concede para someter su tesis a examen profesional, misma autorización que sólo podrá otorgarse nuevamente, si el trabajo recepcional conserve su actualidad y en caso contrario hasta que haya sido actualizado, todo lo cual será calificado por la Secretaría General de la Facultad.

A T E N T A M E N T E.
"POR MI RAZA HABLARA EL ESPIRITU"
Cd. Universitaria, a 22 de noviembre de 2010

DRA. MARÍA ELENA MANSILLA Y MEJÍA
DIRECTORA DEL SEMINARIO

FACULTAD DE DERECHO
SEMINARIO
DE
DERECHO INTERNACIONAL

100 UNAM

AGRADECIMIENTOS

A DIOS, por mi existencia en el universo.

A LA UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO Y SU FACULTAD DE DERECHO, por aceptarme en su seno, cimentar mi crecimiento profesional y darme una muestra de la voluntad de progreso de mi nación.

A MI MADRE TERESITA, por todos sus desvelos, atenciones, apoyo y comprensión de mis múltiples fallas, problemas y temores, por convencerme de explotar mi potencial, e instruirme en el valor de lo espiritual, por su amor incondicional.

Y MI PADRE ENRIQUE, por enseñarme el valor del esfuerzo y el trabajo duro, por meter en mi cabeza que el estudio es para siempre, "cabeza fría y corazón ardiente" papá.

A MIS MAESTROS DE TODA LA VIDA, Rosa, Guadalupe, Baltasar, Ceferino, por abrirme las puertas del conocimiento y el aprendizaje; al Lic. Juan Emmanuel Vicario Pérez-Moreno y Darío Gómez Nolasco, por darme la oportunidad de iniciar en el ejercicio de la abogacía.

A LA LIC. GRACIELA AMALIA OSORIO VILLASEÑOR, por darme el placer de conocer el Derecho Internacional como solo ella sabe exponerlo y sobre todo por aceptar conducir tan atinadamente este trabajo, a pesar de la distancia y el tiempo.

A MIS TÍOS, Lidia Gutiérrez y Juan Márquez por adoptarme cuando necesite un hogar; a Sahara Hernández por admitirme en su casa y compartir su familia en uno de mis momentos de mayor incertidumbre, gracias por escuchar.

A MIS AMIGOS, Luís, José de Jesús, Juan Antonio y Héctor, por el placer de su compañía y complicidad en todo momento, los llevo en mi alma donde quiera que voy.

A MIS HIJAS FERNANDA Y MICAELA, la luces de mi vida y mi mejor motivo para seguir adelante, gracias por llegar a mi vida.

A MI ESPOSA URSULA, compañera , amiga, amante y confidente, siempre fiel e inquebrantable, tu amor y compañía me permiten dormir tranquilo y despertar cada mañana con fuerza para enfrentar la vida. Gracias por enseñarme nuevamente el valor de la humildad y el amor al prójimo. Te amaré siempre.

ELEMENTOS PARA EL DESARROLLO DE UNA CONVENCIÓN INTERNACIONAL EN MATERIA DE GUERRA CIBERNETICA

ELEMENTOS PARA EL DESARROLLO DE UNA CONVENCIÓN INTERNACIONAL EN MATERIA DE GUERRA CIBERNÉTICA

INTRODUCCIÓN

Es una realidad, las fronteras nacionales se han disuelto en el mar de tecnología y globalización, ya no se puede ser espectador de los movimientos mundiales en cualquier terreno, estamos inmersos en las primeras décadas de la tercera gran revolución mundial; fenómenos y hechos como el Internet, el auge en las técnicas de información y comunicación, el ciberespacio y la trascendencia que tiene en nuestra vidas, el nacimiento de la infoesfera y la posibilidad de una vida dentro de ella, el nacimiento de relaciones, expresiones, e inclusive sentimientos, en una zona virtual; situaciones que poco a poco y casi sin notarlo modifican radicalmente nuestras vidas y las de generaciones futuras.

En las ciencias sociales y particularmente el Derecho, la interacción con la cibernética y la tecnología, ha dado pie a estudios transdiciplinarios que amenazan con cimbrar las bases más sólidas de la ciencia jurídica, en tal forma que afectan conceptos que habían permanecido inmóviles durante décadas y quizá siglos, logrando una maleabilidad no esperada, pero necesaria.

Cuestiones como la Teoría del Estado, el nacimiento y auge del Derecho de la Información, la Teoría de Sistemas, la Integración Económica, el Derecho de la Informática, inclusive la soberanía, han encontrado en su interacción con la tecnología, un refugio que les permite crecer y nutrirse para dar vida a nuevas instituciones, nuevas normas y un nuevo orden jurídico mundial.

Especial mención requieren los Derechos Humanos, -entendidos como facultades, prerrogativas o exigencias del ser humano ya sean sociales, económicas, o de cualquier índole, y exigibles frente a cualquier poder público o privado-, mismos que han tenido un avance sin precedentes en su desarrollo, a la par de los fenómenos de la ciencia y la técnica, dado que ambos son expresiones de la cultura y el conocimiento.

En este trabajo, se intenta analizar con el mayor detalle posible, la Guerra Cibernética, como concepto e institución, que a pesar de su carácter antijurídico, representa el método más acabado de presión política y estrategia militar de la actualidad, basta con revisar notas de periódicos, revistas o simplemente ingresar a la red mundial de Internet para darse cuenta de que el fenómeno existe y va en aumento.

En un mundo integrado, poco sorprende que los ataques y las fricciones entre Estados se han vuelto norma, la intervención de sistemas, el control de la información y las comunicaciones forman parte fundamental de la estrategia de los protagonistas de la Guerra Cibernética.

La proliferación de intervenciones de redes y sistemas han forzado a los Estados a aumentar la vigilancia en el ciberespacio, para prevenir esta amenaza. Actualmente dichos ataques son menos que sitios de Internet inservibles, robo, destrucción y corrupción de la información, pero es totalmente seguro que estos ejercicios no son más que la simiente de ataques dirigidos a infraestructura estratégica.

Representa una variación del fenómeno de la guerra misma, con un nuevo campo de batalla, nuevas implicaciones, principios e inclusive derechos. Su lugar se encuentra en el Ius in Bello, dado que se refiere principalmente a medios diversos para llevar a cabo la agresión.
ficticio
Inclusive ya existen situaciones que cada semana, cada día, se presentan ante nuestros ojos, basta con vigilar los tabloides para verificar que son hechos y situaciones muy reales que cada vez están más cerca de ser considerada como un peligro para todos y cada uno de los países que acceden al espacio cibernético.

El fenómeno genera millones de dólares en perdidas sin dejar de lado el enorme número de personas que afecta, en pocos años veremos sin lugar a duda enfrentamientos entre Estados derivados de todo tipo de fricciones políticas y económicas.

Inicia esta labor con la descripción del nacimiento de Internet y su particularidad como hecho jurídico, se establecen principios y analiza la forma jurídica de su estructura, al tiempo que se citan normativas diversas y el avance de la Informática y su importancia para la comunidad internacional, incluidos los logros de Naciones Unidas al respecto con su trabajo en la Cumbre Mundial de la Sociedad de la Información.

El siguiente capítulo es un esbozo de la guerra como institución humana y sus características jurídicas, el análisis que ha sufrido por parte del Derecho en cuanto a su naturaleza, relacionándolo con las nuevas tecnologías y sus medios comisorios más acabados.

El tercer capítulo analiza en primer término el concepto de cibernética, con el fin de adecuarlo a las instituciones bélicas y lograr la caracterización y definición del motivo de la tesis, la Guerra Cibernética, al tiempo que se mencionan algunas particularidades y situaciones relevantes.

El último capítulo comprende el desenlace de este estudio, donde se exponen las bases o principios bajo los cuales se propone opere el estudio y desarrollo de la Guerra Cibernetica en la comunidad internacional, se pugna por la participación de todos los actores del ciberespacio y el desarrollo de conceptos de vital importancia para lograr un justo equilibrio en el nuevo orden propuesto.

Se cree de forma definitiva, que este nuevo acontecer dará un vuelco a las relaciones internacionales, obligará al mejoramiento de las instituciones y llevará a un avance que modifique para bien el Derecho y en particular el Internacional Público.

Hace más de dos años se inicio este trabajo, con la firme convicción de dar vida a un tema poco conocido, realizando el intento inclusive de ser propositivos en su elaboración, y alejarse de este modo de las formas tradicionales del análisis jurídico.

El 1 de febrero de 2010, el Presidente de los Estados Unidos de América, Barack Obama, en su Proyecto de Presupuesto para la Defensa 2011, ha reconocido públicamente al ciberespacio como nueva zona de conflictos, situación que lejos de generar desanimo por el tiempo invertido en este estudio, forja fuerza, ahora con la seguridad de que en los años venideros, este tema estará en boga y con muchos matices aún por descubrir.

Puerto Vallarta, Jalisco a 20 de Septiembre de 2010

1. DERECHO, INFORMÁTICA E INTERNET

1.1 Nociones Preliminares

Para poder entender en su debida extensión las posibilidades y desafíos, que para la ciencia del Derecho ofrecen las nuevas tecnologías, es necesario contar con algunas ideas básicas.

En principio se debe aceptar que el nacimiento y desarrollo de las tecnologías de la información durante los últimos 60 años ha sido vertiginoso, actualmente las fronteras de los Estados parecen por momentos desaparecer en virtud del mar de técnicas que han superado el alcance de los sistemas de orden humano, y como motor de este avance se presentan la Información y la Comunicación; conceptos netamente sociales, cuyo estudio concierne al Derecho.

Lamentablemente, para los juristas es difícil competir con la velocidad a la que se desarrolla la ciencia y la tecnología, problema que obedece en gran medida al temor de los mismos abogados que evitan el estudio de otras ramas del conocimiento, y creen que el Derecho es determinado por sí mismo, y olvidan que esta ciencia tiene su raíz en la realidad histórico social de la conducta y relaciones humanas.

De esta forma es complicado comprender la precocidad de las nuevas generaciones que han nacido bajo el auspicio de la integración de conocimientos y tecnologías, en una relación indisoluble.

En el mismo orden de ideas, México carece de una regulación específica o reconocimiento de instituciones para las nuevas tecnologías, -aunque existen excepciones de alcance técnico que comprende materias como la financiera, telecomunicaciones y el aprovechamiento de los ordenadores para el mejor tratamiento de datos, tal como sucede en registros públicos, juzgados, despachos, casos que únicamente abarcan cuestiones administrativas y

comerciales- en gran medida existe un nivel muy bajo de estudio y explotación con respecto a esta problemática.

En el ámbito internacional, la inferioridad que tienen los países dependientes y atrasados en relación con las potencias mundiales en los rubros de ciencia y técnica, provoca enormes demoras en los estudios sociales, a pesar de que existen iniciativas muy loables que tienden ha reducir e inclusive eliminar la "Brecha Tecnológica", que separa los niveles de desarrollo.

En específico, el nacimiento y desarrollo de Internet, comprende un hecho extraño para los estudiosos del Derecho en su mayoría, ya que existe una tendencia natural a dejar de lado la tecnología para ingenieros, técnicos, llegando al grado de creer que es algo insólito en las humanidades.

Este hecho permea todos y cada uno de los aspectos de nuestra vida, a la par de la globalización, el libre flujo de información y comunicaciones, ha logrado mantener el ritmo de desarrollo que la humanidad posee tras los últimos 25 años.

Así mismo es importante señalar que el área donde adquiere vida este hecho, de características espaciales y temporales ajenas en su totalidad al mundo tangible, conocido popularmente como "ciberespacio", es la conjugación de múltiples áreas del conocimiento, tales como la Cibernética, la Informática, las Comunicaciones, la Economía, la Psicología, la Sociología, las ciencias exactas en general y por supuesto el Derecho.

Esta situación se refleja en las cuestiones de aplicación espacial y temporal de la ley, sujetos, tratados internacionales, contratos mercantiles, comercio en línea, delitos que tiene como medio de comisión los ordenadores, flujo de datos entre Estados, protección de datos personales, libre acceso a la información, derechos de autor, derechos humanos como la libertad de expresión, el respeto a la intimidad, y por supuesto conflictos armados entre Estados.

Ante esta nueva situación el Derecho debe ofrecer nuevas alternativas, visiones más amplias de la realidad, atender por ejemplo a lo que establece el profesor Andrés Botero Bernal:

"Creer que el Derecho se define a sí mismo, sin necesidad de recurrir a otras disciplinas y referentes, es pretensioso y además es un acto de ingenuidad. La disciplina jurídica es un proceso histórico mediante el cual una esfera del saber sociopolítico se sistematiza y organiza, se especializa, y construye progresivamente un objeto y un método hasta ser, finalmente, canonizada (o aceptada) por varios colectivos sociales con capacidad de administrar una verdad en su razonamiento, siendo entonces calificada como tal, una disciplina." [1]

En este caso será ocioso tratar de establecer normas para cada hecho o acto que permita el desarrollo tecnológico, por el contrario, es necesario un nuevo método que diseccione cada situación bajo la luz de la más variada gama de ciencias, distintas áreas del conocimiento que expliquen de forma detallada las nuevas condiciones que enfrentamos y permitan una integración fluida a la conducta social y por ende a la ciencia.

La posibilidad que para los juristas ofrecen las nuevas tecnologías bajo la luz de las ciencias y el Derecho, delimitados pero integrados, son infinitas.

1.2 La Informática y su relación con el Derecho

La Informática, producto de la unión entre Cibernética y Electrónica, nace después de la Segunda Guerra Mundial como parte de la tendencia automatizadora que se presentaba debido a la Guerra Fría, tiempo en el cual se busca una forma más eficiente de archivar, almacenar, transferir y utilizar los grandes flujos de información que permitieran a los países en pugna colocarse por encima de su contraparte; para ampliar esta idea debemos entender información como:

[1] BOTERO BERNAL, Andrés, "Los retos del jurista internacionalista en la contemporaneidad", en Anuario Mexicano de Derecho Internacional , Vol IV, México , 2004 Pág. 254

" conjunto de mecanismos que permiten al individuo retomar los datos de su ambiente y estructurarlos de una manera determinada, de modo que le sirvan como guía de su acción"[2]

Muy a pesar de que Informática y Cibernética constituyen ciencias distintas, es imperativo conocerlas ya que se mencionan de manera recurrente siendo objetos ineludibles para este estudio. En principio es necesario tomar en cuenta a la primera, a fin de delimitar su campo de acción. De acuerdo al maestro Fix Fierro, la Informática es:

> "…la ciencia del tratamiento automático o automatizado de la información, primordialmente mediante las computadoras."[3]

Dicho de forma más clara y concreta la *Informática es la ciencia que estudia y desarrolla los métodos para el mejor procesamiento y aprovechamiento de datos.*

Del adelanto de esta ciencia nace la era de la información, producto del desarrollo de los países poderosos y las grandes corporaciones, benéfica en si misma, ya que su capacidad de penetración en la vida cotidiana, hechos como la digitalización y consulta de textos, hasta el Internet, serían inimaginables sin ella, más sin embargo creadora de conflictos, ya que la información produce poder para el que la detenta y sabe utilizarla en su beneficio.

"…las derivaciones de la Revolución Informática trascienden en todos los campos, abren nuevos horizontes hasta desconocidos, pues la información conduce al poder, afecta sus relaciones , soberanía, equilibrios, economía, elementos de la crisis, por lo tanto dan pauta a una nueva sociedad; pues el establecimiento de una red de comunicaciones a nivel internacional brinda poderío a los Estados."[4]

---

[2] Definición citada en la Cátedra de "Derecho de la Información" por el Lic. Alcalá Méndez Federico F. Ciudad Universitaria, México, Marzo 2007

[3] FIX FIERRO, Héctor, "Informática y Documentación Jurídica", UNAM, Facultad de Derecho, México, 1990, Pág. 43 citado por RIOS ESTAVILLO, Juán Jose, "Derecho e Informática en México", UNAM Instituto de Investigaciones Jurídicas, México 1997, Pág. 5

[4] MEZA SALAZAR, Martha Alicia, "Estado Telematico y Teoría del Estado", Ed. Martha Alicia Meza Salazar, México 2006, Pág. 57

De este modo, la informática representa un campo ineludible para toda ciencia que requiera mejorar los procesos de comunicación e información, se piensa que su crecimiento exponencial depende en gran medida del grado de apertura cultural que los Estados han logrado en la segunda mitad del siglo XX y la primera década del XXI.

Entonces sería una falacia afirmar que el Derecho es ajeno a las relaciones con esta nueva ciencia, tan es así que su combinación da lugar al desarrollo de una rama de reciente creación, el Derecho Informático, misma que carece de una definición particular pero posee un objeto bien definido, el estudio del archivo, almacenaje, transferencia y uso de datos, realizado en su mayoría mediante el uso de ordenadores.

Este nuevo Derecho se divide a su vez en dos vertientes, Informática Jurídica y Derecho de la Informática.

La primera desarrolla los mejores medios para el tratamiento de la información jurídica, realizando esta tarea en 3 fases ampliamente conocidas en la doctrina: *Informática Jurídica Documental* (almacenamiento y recuperación de textos jurídicos) , *Informática Jurídica de Gestión* (principalmente en el área administrativa como Registros Públicos, Certificaciones de documentos provenientes de bancos de Datos, en el ámbito judicial para la automatización de procesos y procedimientos) y *Informática Jurídica Metadocumental* (apoyo en toma de decisiones, actividades Fedatarias, educación, investigación , redacción).[5]

En cuanto a la segunda, el Derecho de la Informática se dedica al estudio y resolución de los problemas jurídicos que el uso de la informática produce, para el efecto existen diversos puntos sujetos a desarrollo por parte de los estudiosos de la doctrina, mismos que por si solos son objeto de trabajos particulares, por lo que únicamente se citan de manera enunciativa, sin limitarse a ellos exclusivamente:

- Regulación de bienes informáticos (propiedad de la información que circula por redes).
- Protección de datos personales.
- Flujo de datos transfronterizos

[5] TELLEZ VALDEZ, Julio, "Derecho Informático", UNAM, México, 1991, Págs. 14-41

- Derechos de autor (propiedad y aprovechamiento de programas de computo).
- Delitos informáticos.
- Comercio y contratos.
- Valor probatorio de documentos provenientes de redes.
- Ergonomía informática (cuestiones de orden laboral)[6]

Como se puede apreciar, el Derecho esta intrínsecamente ligado a la Informática, en tanto que el primero se nutre de flujos crecientes de información, y se ve beneficiado por las bondades de los datos que proporciona su mejor procesamiento. La disciplina jurídica esta en constante estudio de los problemas que derivan de la aplicación de la automatización a los datos.

1.3 Internet como Hecho Jurídico

Ya durante las décadas de los sesenta y setenta el estudio y desarrollo de redes para compartir información de terminales de ordenadores (realmente existe nula diferencia entre el termino ordenador y computadora, únicamente su origen es distinto, más tienen el mismo significado), era una realidad, auspiciada por el gobierno de los Estados Unidos de América, en especial las dependencias militares.

Se desarrolló en los cuarteles de la Agencia de Investigación de Proyectos Avanzados del Pentágono, un sistema que permitía enviar grandes cantidades de información de una computadora a otra en un tiempo relativo corto, dicho sistema se denominó ARPANET.

Dada la cantidad de inversión necesaria para el desarrollo de tecnologías nuevas, y con plena Guerra Fría en proceso, se decidió avanzar en el desarrollo de este medio mediante la inversión privada, las corporaciones entraron al proyecto, al igual que los ingenieros de todo el país y algunas universidades que podían pagar el costo de establecer terminales en sus campus.

[6]TELLEZ VALDEZ, Julio, "Derecho Informático", *Op. Cit.* págs. 41-98

El resultado fue el crecimiento exponencial de este sistema que de la mano con la reducción de costos en los equipos de cómputo y el desarrollo de mejores medios de comunicación entre ordenadores, se produjo una revolución en la información, su manejo y procesamiento.

Siguiendo lo doctrina francesa del hecho jurídico en sentido estricto, es:

"…todo aquel acontecimiento natural o del hombre generador de consecuencias de derecho, no obstante que cuando proviene de un ser humano, no existe la intención de crear esas consecuencias."[7]

Para el maestro Eduardo García Máynez, el hecho jurídico implica acciones del hombre de tipo lícito que:

"…tienen por finalidad la creación, la modificación, la transmisión o la extinción de consecuencias de derecho,…" [8]

Para este autor, la diferencia entre hecho y acto, estriba en que el primero se refiere a consecuencias y el segundo a derechos y obligaciones. Entonces si se analiza el Internet bajo esta perspectiva, existe un hecho, ya que por si mismo, es ajeno a la creación, modificación, transmisión o extinción de un derecho u obligación, soslaya tanto la adjudicación de potestad a un sujeto como la vinculación para exigir de otro un dar, hacer o no hacer. Por el contrario, si produce consecuencias jurídicas, ya que involucra un resultado que afecta la esfera jurídica de los sujetos.

La afirmación de Internet como hecho, esta justificada en virtud del aspecto histórico del mismo, ya que su creación responde en total medida a un deseo humano, que era en principio un medio para el mejoramiento de los procesos mediante los cuales se recopilaba y encausaba la información a fin de utilizarla

[7] DOMÍNGUEZ MARTINEZ, Jorge Alfredo, "Derecho Civil Parte General. Personas. Cosas. Negocio Jurídico e Invalidez", Ed. Porrúa, 8ª Edición, México 2000, Pág. 501
[8] GARCÍA MÁYNEZ, Eduardo, "Introducción al estudio del Derecho", Ed. Porrúa, 58ª Edición, México 2005, pág. 183

en los procedimientos de inteligencia militar y científica, que provocó consecuencias de derecho, inesperadas en la forma que se produjeron.

Estas consecuencias, por ejemplo, abarcan desde la comisión de conductas que ahora son consideradas como delitos, tal es el caso de el acceso ilícito a sistemas informáticos, entre los que pueden destacar el robo a instituciones financieras o redes de defensa; así como el uso indiscriminado de programas libres de transferencia de datos entre usuarios que permiten el libre intercambio de material de video, sonido, escrito, informático, dando un vuelco a la regulación en materia de derechos de autor. Otrora situaciones impensables, ahora hechos comunes.

Existen algunas aproximaciones a una conceptualización de Internet, por ejemplo:

"…Internet es una red mundial descentralizada que une redes, que a su vez conectan computadoras u ordenadores."[9]

En concreto, el Internet es un término que nace de forma lógica, las interconexiones entre redes independientes fue llamada *Internetwork*, la contracción inglesa lo estableció como *Internet*, actualmente se entiende en forma amplia como:

"…la Asociación Global de computadoras que llevan datos y hacen posible el intercambio de información…"[10]

Como se aprecia existe gran similitud entre las nociones propuestas, aunque es pertinente recalcar que esta asociación permite *el flujo continuo de comunicaciones en tiempo real,* en virtud de que la información implica el análisis y uso de datos con los cuales respondemos a los estímulos del ambiente, es decir un proceso personal interno y la comunicación comprende la

[9] FERNANDEZ RODRÍGUEZ, José Julio, "Lo Público y lo Privado en Internet. Intimidad y libertad de expresión en la Red.", Instituto de Investigaciones Jurídicas, UNAM, México, 2004, Pág. 1
[10] PARDINI, Anibal A., "Derecho de Internet", La Rocca, Buenos Aires, 2002, Pág. 96 citado por GARCIA BARRERA, Myrna Elia , "Derecho de las Nuevas Tecnologías", UNAM Instituto de Investigaciones Jurídicas, México 2008, Pág. 44

exteriorización del pensamiento por medio de un canal con el fin de provocar en otro una respuesta.

Esta asociación de ordenadores es producto de la participación de innumerables personas, dependencias y asociaciones, civiles, militares y particulares, que constituyen un elemento material y activo, ellos produjeron el hecho, más en cuanto a los resultados obtenidos, se entiende una actitud pasiva de todos los sujetos inmersos en el proceso, en una frase, esta diseñado por todos y para todos sin esperar los resultados obtenidos; existe entonces oposición a los actos volitivos, faltó consenso respecto de su creación, la finalidad esperada se situó lejos de las consecuencias que tanto en el mundo general como el jurídico, provocó.

Si bien es cierto el Internet solo es una parte de las llamadas nuevas tecnologías, para el tema de la Guerra Cibernética, tiene una importancia toral, debido en gran parte a que este es el medio idóneo para desarrollar dichas actividades, sin que las mismas se limiten a este espacio.

1.3.1 Principios

Uno de los grandes problemas para la negociación de tratados internacionales o simplemente la creación de leyes locales que regulen o delimiten tecnologías como el Internet, es precisamente la incomprensión en cuanto a su funcionamiento, por tal motivo es necesario instaurar que este hecho, al conformar el medio de comunicación y transmisión de información de mayor crecimiento, produce consecuencias tanto políticas, como sociales y jurídicas, es por ello que esta investigación pretende establecer bases para su mejor entendimiento:

- *Libre Asociación Global.* Durante la primera mitad de la década de los noventa, específicamente el 24 de octubre 1995, se realizó una magna reunión de miembros ligados a la creación y desarrollo de Internet, auspiciada por la *National Science Foundation*, donde se estableció la concepción más aceptada y reconocida por los expertos, misma que retomamos para este trabajo:

"El sistema de Información Global que:

1.- Se encuentra Vinculado lógicamente por su espacio direccionable global determinado basado en el Protocolo de Internet (IP) o sus subsecuentes extensiones y agregados.
2.- Es Capaz de soportar comunicaciones utilizando un conjunto de herramientas de Protocolo de Control de Transmisiones / Protocolo de Internet (TCP/IP) o sus subsecuentes extensiones y agregados.
3.- Provee, utiliza o hace accesible, en forma pública o privada, servicios de alto nivel estratificados en las comunicaciones y en la infraestructura relacionada aquí descrita"[11]

El Internet contiene una cantidad enorme de redes propiedad de distintos usuarios, que se conectan entre si pero carecen de una autoridad central, el sistema opera de acuerdo a los aportes de miles de personas e instituciones, que en principio solo obedecen los lineamientos técnicos del lenguaje que hace posible la comunicación entre tantas maquinas, el *TCP/IP* o *Transmision controler protocol/Internet protocol,* estas reglas permiten repetir procesos una y otra vez sin equivocarse, en particular, el *TCP/IP,* sirve para descomponer en partes la información que se envía, numerar esas partes, empaquetarlas y enviarlas a la dirección propuesta, así el ordenador que las recibe al manejar el mismo lenguaje, puede desempacar esos datos y estructurarlos con la misma facilidad para que el mensaje sea comprensible.

- *Intangibilidad de su espacio*. El ciberespacio lo conforman la interconexión de las redes, el contenido, la información, los sitios que la presentan y las herramientas que permiten la comunicación, en un mundo virtual, que existe pero no es palpable.

- *Inmediatez de sus actividades*. El tiempo en que se desarrollan es real o inmediato, ya que las transferencias de información y comunicaciones se dan en modo casi instantáneo, y derivan en problemas jurídicos como el del ámbito de validez o aplicación de la ley, además, mantiene un crecimiento exponencial en cuanto a su evolución, aproximadamente 7 veces más rápido que el mundo tangible.

[11] GARCIA BARRERA, Myrna Elia , "Derecho de las Nuevas Tecnologías", *Op. Cit.* pág. 40

- *Exacerbación de libertades en oposición a la regulación del Estado*. Los gobiernos están impedidos para regular y siquiera definir que es este nuevo espacio, por tal situación las libertades del hombre son casi ilimitadas, en parte gracias a la facilidad con que se obtiene el anonimato dentro del sistema, así la libre información, expresión, comunicación, transito (capitales, servicios), intimidad, igualdad constituyen un nuevo bastión para esconderse del mundo real. Inclusive hay quien asegura que esta entidad pone en peligro el equilibrio de la paz en el mundo. Aunque a ultimas fechas son más y más las leyes y los países que pretenden regular su contenido.

- *Inexistencia de Fronteras.* Las delimitaciones territoriales para los Estados, son inaplicables al Internet, a pesar de que los proveedores de servicios, la información y las consecuencias de su aplicación tienen un soporte material en algún lugar, las conexiones virtuales y la comunicación entre las computadoras desobedecen las divisiones físicas. Existe la posibilidad de acceder a cualquier base de datos de un país determinado, a las paginas de contenido, inclusive sistemas restringidos sin la necesidad de un permiso especial, estos sistemas solo requieren que los ordenadores obedezcan reglas técnicas uniformes, sin importar el origen de la solicitud de ingreso o la nacionalidad del usuario.

- *Mutabilidad*. La red de redes esta en constante cambio y evolución, ya que si bien es cierto que su lenguaje madre es básico, el acceso e intercambio de información, esta sujeto a múltiples variables, tanto físicas como virtuales, ya sea el soporte material, la maquinaria o el software, los programas. Cada persona que ingresa, produce un cambio y varia las condiciones del sistema, es así que la capacidad del Internet debe crecer de manera continua, al igual que mejorar la rapidez de las comunicaciones entre los nodos que la conforman.

- *Ciudadanía cibernética.* Los autodenominados *netizens* son los ciudadanos del Internet, inclusive existen declaraciones de independencia del Internet, que lo señala como un espacio libre de la mano y regulación de

Estado alguno, situación que queda de manifiesto en la instauración de redes sociales proporcionadas por diversos proveedores como *Facebook* o *Twitter,* mismas que permiten la comunicación sin restricciones, así como redes privadas que pugnan por el reconocimiento de sus fines en el mundo físico, aquí podemos apuntar que el Internet es solo un medio, nunca fin, el que exista esta reclamación de respeto a un derecho como la ciudadanía, deriva de la exigencia de la sociedad creada en la infoesfera para defender el libre acceso sin restricciones dentro del ciberespacio.

- *Libertad de acceso*. Cualquier persona en el mundo puede ingresar al ciberespacio, sin más limitaciones que los requerimientos técnicos mínimos que el propio sistema impone. Actualmente esta situación que en muchos países se pretende sea reconocida como derecho humano manifiesta diversas barreras que impiden la entrada a Internet, tales como la falta de equipo, escaso conocimiento de su funcionamiento, desconocimiento del lenguaje (ya que el 70% se presenta en ingles), poco interés, miedo a las nuevas tecnologías, limitaciones a derechos políticos como libertad de información, expresión, privacidad, así como los términos estándar internacionales para el acceso a través de uno de los trece servidores raíz en el mundo.

Ejemplo, en un ejercicio analógico, el ciberespacio tiene 13 puertas de entrada situadas alrededor del mundo y representadas físicamente por enormes servidores, máquinas que controlan el flujo de datos entre computadoras. Cualquier ordenador que desee acceder a esta red mundial lo hace a través de una de estas, para ello debe cumplir con los requerimientos mínimos técnicos de lenguaje, compatibilidad, identidad, seguridad, entre otros.

- *Concepto.* Internet es *la Libre asociación de redes autónomas de ordenadores que tiene como fin la transmisión de información y comunicación sin estar sujetos a un sistema de control global o local particular*.

1.3.2 Aplicación de la Ley.

Al hablar de validez de una norma es necesario tener en cuenta que el fin de todo ordenamiento jurídico es que se aplique, que la propia sociedad que se sujeta a ese sistema de control entienda como obligatoria la norma y la cumpla, que ajuste su conducta a dicho precepto, en otras palabras que sea *eficaz:*

"Afírmáse, que un imperativo es *eficaz*, que tiene *facticidad* o *positividad,* cuando es acatado por los sujetos a quienes se dirige." [12]

Por su parte el internacionalista Botero Bernal al hablar sobre eficacia nos señala:

"Se tomará por eficacia la conformidad de la conducta social con la conducta motivada por la norma."[13]

Si esta relación de *norma - conducta* se da, se puede decir que la norma es eficaz, pero si carece de esta correlatividad, carece de sentido, muy a pesar de ser válida, ya que en si misma es inaplicable.

En este momento es adecuado señalar la diferencia entre validez y eficacia a fin de evitar confusiones, el primer concepto se refiere al proceso formal que debe seguir el legislador al crear una norma, una norma válida será la que cumpla con los requisitos de este proceso, por su parte la eficacia debe comprenderse como la reciprocidad entre lo establecido en la norma con las acciones de los sujetos que regula.

Para este análisis, se utiliza la clasificación Kelseniana de los cuatro ámbitos de validez de la norma:

[12] GARCÍA MÁYNEZ, Eduardo, "Introducción al estudio del Derecho", *Op. Cit*. Pág 7
[13] BOTERO BERNAL, Andrés, "Los retos del jurista internacionalista en la contemporaneidad", *Op. Cit.* Pág. 257

"El ámbito de validez de las normas del derecho debe ser considerado, según Kelsen, desde cuatro puntos de vista: el *espacial,* el *temporal,* el *material* y el *personal.* El ámbito *espacial* de validez es la porción del espacio en que un precepto es aplicable; el *temporal* está constituido por el lapso durante el cual conserva su vigencia; el *material*, por la materia que regula, y el *personal,* por los sujetos a quienes obliga"[14]

El ámbito espacial comprende el lugar limitado en que un ordenamiento jurídico expedido conforme a un proceso legislativo debe surtir sus efectos. En el caso de los Estados, sus leyes internas se circunscriben a su propio territorio. En nuestro país existen leyes federales, locales y municipales; esta clasificación aunque general es aplicable perfectamente al Derecho Internacional Público, ya que la propia jurisprudencia ha establecido la jerarquía correspondiente a las normas de derecho uniforme internacionales, proporcionándoles una zona de acción, colocándolas en el mismo nivel que nuestra constitución excepto cuando vayan en contra de esta.

El ámbito temporal tiene que ver con la vida misma de la norma, la vigencia, el periodo en que es válida y susceptible de eficacia, lapso que varia de acuerdo a la norma de que se trate, sea una ley expedida por el Congreso de la Unión o una resolución jurídica que son vigentes a partir de su publicación por ejemplo y concluyen con su derogación, abrogación o cumplimiento, según sea el caso. El propio maestro Máynez al hablar de la vigencia del orden jurídico establece:

"… conjunto de reglas impero – atributivas que en una época y lugar determinados el poder público considera obligatorias."[15]

El ámbito material se refiere al área especializada del Derecho que rige la norma, en la división clásica del Derecho Objetivo, se encuentra el Derecho Público que regula las relaciones donde el Estado es uno de los sujetos del citado vínculo y normas de Derecho Privado donde los sujetos tendrán el carácter de particulares. El profesor Alberto F. Senior al respecto señala:

[14] KELSEN, Hans., "El Contrato y el Tratado", México, 1943, Pág. 953 citado por GARCÍA MÁYNEZ, Eduardo , "Introducción al Estudio del Derecho", *Op. Cit*, Pág. 80
[15] *Ibidem,* Pág 97

"…LAS NORMAS DE DERECHO PÚBLICO, se caracterizan en que el Estado constituye uno de los elementos de la relación jurídica. Las segundas; o sea, las normas de DERECHO PRIVADO, son aquellas en las que el Estado no forma parte como uno de los elementos de la relación jurídica, que la norma establece." [16]

Para el caso las normas del Derecho Internacional Público pertenecen al primer grupo, dado que los Estados actúan como sujetos en la relación jurídica que el orden cita.

Por último, el ámbito personal de la norma de acuerdo al jurista García Máynez, debe ser comprendida dentro de dos esferas.

La normas *genéricas* y las *individualizadas,* las iniciales comprenden a todos los que se ubiquen en el supuesto normativo de forma abstracta, las segundas, obligan o facultan a uno o varios sujetos determinados, de forma concreta. Las normas individualizadas se dividen en públicas y privadas, las primeras proceden de la voluntad de los particulares y las siguientes de la actividad del Estado. [17]

De acuerdo a Máynez, los tratados internacionales son normas individualizadas públicas, ya que se refieren a sujetos determinados que acuerdan voluntariamente, en tanto son sujetos de derecho internacional, la aplicación de una norma consensual.

Dentro de los cuatro ámbito de validez de la norma, el espacial y el temporal son de capital importancia para el Internet.

En principio, la validez espacial, constituye tal vez el mayor de los problemas que impiden su sujeción a un cuerpo normativo, principalmente se debe poner atención al principio de intangibilidad de su espacio, ¿cómo puede un solo Estado fijar pautas o regular determinadas actividades en un espacio virtual?.

Primero es menester tratar de conceptualizar que es *Espacio Informático, Virtual o Cibernético*:

[16] SENIOR, Alberto F. , "Filosofía del Derecho", S.E. , México 2008, Pág. 44
[17] GARCÍA MÁYNEZ, Eduardo, "Introducción al Estudio del Derecho", *Op. Cit.* págs. 82-83

"Infraestructura electrónica cuyos componentes son bases de datos múltiples, redes de transmisión de datos y sistemas de información y de consulta. Miles de bases de datos conteniendo información de todos los rincones de la Tierra ligados en red y red de redes en continua expansión y uso permanente. Esta infraestructura electrónica es el sostén electrónico de la infraestructura que alimenta el proceso de toma de decisiones. Es en consecuencia: el conjunto integrado por tecnologías electrónicas y el conjunto de información que alimenta sus actividades, transacciones, negocios, contratos, ordenes, instituciones, maniobras, transferencias, transmisiones de información, datos, conocimientos, delitos, fraudes, promesas, mentiras, buenos consejos, controles, investigaciones científicas, etc. Realizados a través de las redes de transmisión de datos y telecomunicaciones, y de las redes de redes, en el mundo entero en tiempo real." [18]

Otro concepto propuesto por el investigador José Julio Fernández Rodríguez para el ciberespacio es:

"El *ciberespacio* es un concepto más amplio al aludir a toda la red informática que une el mundo a través de los más variados soportes, sean terrestres o aéreos. El ciberespacio es el espacio artificial resultado de Internet y de otros avances informáticos. Se trata de una realidad virtual y no física. El concepto fue acuñado en 1984 por William Gibson en su novela fantastica *Neuroromancer,* en donde se describe el mundo de las computadoras y la sociedad creada en torno a ellos".[19]

Sirva esto como acotación, en virtud de que el uso de las palabras Informática y Cibernética, si bien tienen gran diferencia conceptual, se han homogeneizado, y como resultado existen ahora términos con el mismo significado, por ejemplo: espacio informático, ciberespacio, espacio cibernético, redes cibernéticas, redes informáticas.

En esta investigación el termino ciberespacio se entenderá como la *zona artificial creada por la interconexión de las redes mundiales de información y comunicación.*

[18] RÍOS ESTAVILLO, Juan José , "Derecho e Informática en México", *Op. Cit*., pag. 70
[19] FERNANDEZ RODRÍGUEZ, José Julio, "Lo Público y lo Privado en Internet. Intimidad y libertad de expresión en la Red.", *Op. Cit*., Pág. 2

Las fronteras del Internet como hecho, distintas a la particularidad territorial de los Estados, carece de características geográficas o líneas tangibles, pero existe cierto grado material para su soporte, dado que se ingresa a el mediante el uso de un ordenador y un prestador de servicios de Internet (ISP) que necesariamente sujeta el otorgamiento de esta prestación a un determinado cuerpo normativo

Por ejemplo Teléfonos de México se debe sujetar a lo estipulado en la concesión que se le ha otorgado, el mismo tiene reglas de uso para el servicio que proporciona, de la misma forma el uso de programas de cómputo e inclusive el acceso a portales de la misma red, están siempre condicionados al cumplimiento de cierta normatividad, que a fin de cuentas regulan la actividad de los usuarios.

El problema de la aplicación de la ley en el espacio que representa la Internet se resume en ¿como sujetar a los individuos al cumplimiento de normas jurídicas en un espacio común, donde son inexistentes los Estados y el orden como lo conocemos?, ¿cómo lograr eficacia en dichas normas?

Por otro lado, el ámbito de aplicación temporal, dentro de este sistema, es inoperante si se tiene como base la premisa de que la norma jurídica solo tiene eficacia desde que entra en vigor, se publica la resolución o se acuerda entre las partes.

Una norma local, en cualquier Estado, emitida con el fin de regir a partir de un tiempo determinado, es insuficiente para cubrir la complejidad de las relaciones cibernéticas en la red, dado que el número de supuestos que dicho ordenamiento debe cubrir es tan amplio que el mismo crecimiento vertiginoso del Internet dejaría cualquier ley en calidad de obsoleta, inclusive antes de ser publicada.

A pesar de que en la vida profesional se comete el error de creer que solo la norma jurídica o el Derecho es el único sistema de control de conducta, se debe tener presente que el Internet se auto-regula, ya que cada ordenador y

cada persona detrás, esta vigilando y supervisando nuestras actividades, ello sin contar a los propios proveedores de servicio, organizaciones civiles y científicas, inclusive gubernamentales.

La respuesta al problema de los ámbitos de validez esta más cerca de lo que pensamos, ya que actualmente el Internet posee una innumerable cantidad de acuerdos que constituyen verdaderos actos jurídicos, que si bien son incoercibles, cada usuario debe respetar.

Por ejemplo, cumplir con la base del lenguaje TCP/IP que permite el acceso al sistema, la normatividad contractual entre proveedores y usuarios, las costumbre comerciales, códigos de buena conducta entre los usuarios de Internet y los servicios ofrecidos por ese medio.

Tal vez es prematuro pensar en preceptos jurídicos escritos o codificación, pero existe eficacia en estas reglas que a manera de normas de trato social, costumbre o simplemente usos, se han mantenido a pesar de sus diferencias.

Las primeras comprenden un tipo de convencionalismo social que representa reglas de conducta externa ajena a la norma jurídica, es decir distinta en cuanto que el convencionalismo posee naturaleza unilateral y la sanción que lo acompaña no está determinada, contrario a la norma de derecho , misma que impone derechos y obligaciones a los sujetos de la relación y la posible sanción esta precisada desde un principio por un ente superior.[20]

Entre ellas y en calidad de ejemplo destacan las llamadas *Netiqueta* que se resumen en*:*

Cortesía. No se debe abusar de una pagina o servicio monopolizándolo,
Prudencia. Cuidado de los servicios y facilidad en su uso.
Evitar envíos sensibles por la red.
Respeto a los derechos de autor.[21]

[20] SENIOR, Alberto F. , "Filosofía del Derecho", *Op. Cit.* , Pág. 55-57
[21] FERNÁNDEZ RODRÍGUEZ, José Julio, "Lo Público y lo Privado en Internet. Intimidad y libertad de expresión en la Red", *Op. Cit.* Págs. 147-148

Su eficacia es inconsistente con sanciones corporales o pecuniarias determinadas por un ente superior, que por su naturaleza exterior condenan las consecuencias del actuar de los sujetos en sociedad, por el contrario en este tipo de convencionalismo, los resultados de las actividades y responsabilidad de cada usuario para mantener las libertades que imperan en el sistema, las conexiones limpias y sin vigilancia, están penados únicamente por la propia sociedad que solo en el momento del quebrantamiento de dicho supuesto establecerá la sanción correctiva necesaria.

Así la conducta se adecua de forma más sencilla y rápida, eliminando la característica coercitiva que al tratar de imponer una sanción requiere de todo un proceso de determinación previo. Además, estos principios son intemporales ya que atienden a las bases sobre las que se funda el mismo sistema y que se modifican a la par de las conversiones técnicas que el mismo sufre, como capacidad, velocidad, acceso a la información.

1.3.3 Finalidad

Hablar de un solo fin del Internet es una tarea complicada, sobre todo si tenemos en cuenta que por su naturaleza mutable cada usuario posee un propósito que busca al momento de ingresar al sistema.

Si hablamos de la finalidad histórica, lo fue la transmisión de información, mediante la libre conexión de ordenadores a la red, hoy en día ha sido rebasada por las posibilidades que nos brinda este hecho.

Para este trabajo, la intención estriba en el análisis del fenómeno como hecho jurídico, sus principios y consecuencias como medio comisorio para la guerra cibernética, situaciones susceptibles de estudio por parte de nuestra ciencia.

Para el sistema económico y político que predomina actualmente en las relaciones internacionales, se ha utilizado en su gran mayoría para la comercialización de bienes, servicios, flujo de capitales, publicidad y propaganda, dada su rapidez, comodidad y bajo costo.

De igual forma, y para muchos Estados en el mundo, la meta será su uso como medio de presión, como uso de la fuerza, cuestión que se analiza en el capítulo siguiente.

Estadísticamente casi el 90% de los ingresos al sistema tienen como fin el comercio. El otro 10% restante son búsquedas de información, desarrollo de investigaciones, mejoramiento de protocolos de Internet, actividades ilícitas.

Para nosotros la finalidad de este hecho aún está por definirse, tal vez porque carezca de una meta o tenga muchas, pero sus consecuencias en el desarrollo de la ciencia y la tecnología, la globalización, el mejor proceso de datos, las libertades de información, expresión, la cultura, los sistemas políticos, económicos, sociales y jurídicos si son concretos, o quizá porque Internet es un medio en si mismo y sería inútil encasillarlo en un fin; en todo caso ha inmerso al mundo en esta nueva etapa de evolución que sería poco probable sin el.

1.3.4 Marco Normativo

Al citar un marco normativo, lo tratadistas intentan ubicar los ordenamientos que regulan tal o cual fenómeno o institución, dado que el hombre gusta de reglamentar todas y cada una de las variables del sistema, inclusive nuestra vida.

Esta tarea es muy complicada, dado que la misma realidad, el conocimiento, la conducta humana, evolucionan constantemente, el problema surge en el momento que esta regulación queda obsoleta y deja de ser eficaz.

Es por esta situación que tratar de enlistar un marco normativo para el Internet, es difícil.

En realidad la cantidad de leyes locales y tratados internacionales que tratan el tema son escasos o nulos, ya que en su mayoría existen leyes y ciertos

acuerdos que regulan principalmente las comunicaciones, y dentro de estas encuadra Internet.

Tratan cuestiones muy particulares, en su mayoría de gobierno electrónico, captación de contribuciones y actividades comerciales, es inexistente una codificación que permita conocer a Internet como hecho y principios que desentrañen su naturaleza a fin de regular su funcionamiento y actividades.

Algunos de los organismos internacionales que han tratado de regular el acceso a las redes informáticas y el tratamiento de la información son los siguientes:

Internet Corporation For Assigned Names and Numbers. Se trata de un organismo de carácter internacional creado por el sector privado en 1998, corporaciones y asociaciones civiles, que se caracteriza por carecer de fines lucrativos, dedicado a coordinar , regular y establecer el Sistema de Nombres de Dominio y las direcciones de Internet, mismas que deben ser únicas para que cada una de las computadoras conectadas a Internet tengan la posibilidad de identificarse unas a otras.

Cada computadora requiere de una dirección electrónica o *IP* (Internet Protocol), una clave que la identifica de todas las demás y permite su ubicación, estas direcciones numéricas son traducidas a lenguaje alfanumérico, es decir letras, a fin de ser recordadas, convirtiéndose así en un Nombre de Dominio, mismo que forma parte de un sistema totalizador regulado por el organismo en cita (*DNS - Domain Name System*).[22]

En un ejemplo ficticio, la dirección electrónica de la página de la Universidad Nacional Autónoma de México es *14.4512.154.12* y su correspondiente Nombre de Dominio *http\\:www.unam.mx,* tecleando en la barra de búsqueda de un programa explorador de Internet cualquiera de las dos formas, permitirá el acceso a la pagina requerida.

[22] FERNÁDEZ RODRÍGUEZ, José Julio, "Lo Público y lo Privado en Internet. Intimidad y libertad de expresión en la Red", *Op. Cit.* Págs. 4-5

Sus beneficios son públicos y sus miembros, diseminados por todo el mundo, personas y asociaciones, se dedican a mantener el Internet seguro, estable y operativo. La *Internet Corporation For Assigned Names and Numbers* promueve la competencia y desarrolla políticas para las identificaciones únicas del Internet.

A pesar de ello, sería inexacto afirmar que controle el contenido del Internet o la red misma, ni siquiera controla el acceso al mismo, pero a través de su rol de coordinar los nombres de Internet, mantiene un alto desempeño en la evolución e impacto de la red.

Para su labor, divide al mundo en regiones determinadas, Europa; Asia-Australia-Pacifico; Latinoamérica-Caribe; África; y Norteamérica, cinco zonas donde se ubican los trece servidores raíz que contienen el sistema de nombre de dominio, encargados del transito de información y comunicación en la red.

Global Business Dialogue and E-commerce. Nace como una estrategia de varias compañías desarrolladoras de tecnología que trataban de evadir ciertas aspectos regulatorios en distintos países.

Es un organismo privado fundado en enero de 1999 con el objeto de desarrollar políticas globales para el mejor crecimiento de la economía en línea. Promueve el dialogo entre lo gobiernos y los sectores privados

Los principales temas de que se ocupa son impuestos; tarifas; encriptación de información; autenticación de usuarios; protección de datos.

Global Information Infraestructure Comission. Organización independiente no gubernamental que involucra a industriales relacionados con las comunicaciones y la información, tanto de países en desarrollo como desarrollados. Fue creada para responder al nuevo paradigma que vive el mundo y para el cual, las instituciones tradicionales y la regulación carece de respuestas adecuadas. Fomenta la discusión sobre cómo las nuevas

comunicaciones, tecnologías de la información, el crecimiento económico, las libertades políticas, impactan la vida local e internacional

Entre sus actividades primordiales están las que se dirigen a la promulgación y adopción de políticas públicas , realización de foros mundiales, estudios conductuales, e intercambio de información, todo encaminado al desarrollo de una sociedad de la información equitativa, sustentable encaminada al bienestar de las personas alrededor del mundo.

Algunos de sus miembros son:

One Communications, BT Group plc, Fujitsu Limited, Mitsubishi Corporation, Economic Commission for Africa, Russian Space Communications Company, Tokyo Electric Power Company, Inc., Harvard University's Kennedy School of Government, Cisco Systems , Telecomunicações de São Paulo Participações , Samsung Electronics, Ford Motor Company , Hitachi , Siemens AG ,Toyota Motor Corporation , Nokia Group, World Bank , Citibank, N.A.

Internet Society. Organización internacional sin fines de lucro fundada en 1992, para proveer una sola línea en los estándares a los que se sujeta Internet. Debe asegurar el desarrollo, evolución y uso del Internet para beneficio de todas las personas alrededor del mundo.

Agrupa a su vez a los cuerpos de expertos responsables de las normas de infraestructura del Internet, arquitectura e ingeniería del mismo, entre ellos , más de 80 organizaciones alrededor del mundo.

Association For Progressive Communications. Fundada en 1990, es una organización no gubernamental y una red internacional que busca que todas las personas tengan acceso a un Internet libre y abierto para mejorar sus vidas y lograr un mundo más justo.

Hoy en día es una asociación sin fines de lucro de más de cinco docenas de redes de miembros y socios en todo el mundo, con el compromiso de asegurar que Internet sirva los intereses y necesidades de la sociedad civil global.

La Unión Internacional de Telecomunicaciones, organismo dependiente de la Organización de Naciones Unidas con sede Ginebra, Suiza, creado en 1992, es el más importante con respecto a las tecnologías de la información y la comunicación; está formada por 191 Estados miembros y más de 700 miembros de sector y asociados

Sus principales actividades se centran en las Radiocomunicaciones, la Normalización y el Desarrollo, donde se abarcan la gestión de los recursos internacionales con respecto al espectro de radiofrecuencias y la órbita de los satélites; creación de normas, y la garantía de un acceso equitativo y asequible a las tecnologías de la información y la comunicación.[23]

En cuanto a Internet esta encargada de la consecución de los objetivos de la Cumbre Mundial de Sociedad de la Información, así como de la emisión de recomendaciones.

La Organización Mundial de la Propiedad Intelectual, con sede en Ginebra , Suiza, parte del sistema de la Organización de las Naciones Unidas, fundada en 1967, su objetivo es desarrollar un sistema de propiedad intelectual internacional, salvaguardando este tipo de derechos personales como lo son, las patentes, marcas, diseños industriales, estimulando de este modo la creación y el desarrollo económico.

Entre sus principales actividades se encuentran la armonización de legislación y procedimientos locales; intercambio de información, solución de controversias, asistencia jurídico técnica en materia de propiedad intelectual. [24]

---

[23] ORGANIZACIÓN DE LAS NACIONES UNIDAS (O.N.U.), UNION INTERNACIONAL DE TELECOMUNICACIONES, "Marco Jurídico" , Abril 2009
http://www.itu.int/net/about/legal-es.aspx

[24] ORGANIZACIÓN DE LAS NACIONES UNIDAS (O.N.U.), ORGANIZACIÓN MUNDIAL DE LA PROPIEDAD INTELECTUAL, "¿Qué es la OMPI?". Abril 2009
http://www.wipo.int/about-wipo/es/what/

En materia de Internet ha desarrollado recomendaciones relativas a cuestiones de propiedad intelectual relacionadas con los nombres de dominio de Internet, es decir las direcciones de los sitios, incluyendo la solución de controversias además de contribuir exhaustivamente en el fomento del uso de nuevas tecnologías para el almacenamiento y acceso a la información en esta materia

Cabe señalar que de manera reciente y especialmente en Europa se han desarrollado proyectos de ley para limitar el trafico de información compartida en redes de usuarios, principalmente para proteger los derechos de autor y las obras legítimas, por lo que estas regulaciones se encaminan a la condena de las descargas ilegales de contenido y tienen como pena la restricción de acceso por tiempo determinado indefinido, situación que se apunta violatoria de derechos humanos.

Comisión de las Naciones Unidas para el Derecho Mercantil Internacional , también integrante del sistema de Naciones Unidas, creada por la Asamblea General de la misma en 1966 mediante la resolución 2205 (XXI) de 17 de diciembre.

Su objetivo principal es la unificación y armonización del Derecho Mercantil Internacional , a fin de lograr una mejor actividad comercial en el mundo.[25]

Entre las pautas relativas al comercio electrónico entre ellas destaca la Ley Modelo de la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional sobre Comercio Electrónico de 1996, que tiene por objeto facilitar el uso de medios modernos de comunicación y de almacenamiento de información, por ejemplo el intercambio electrónico de datos, el correo electrónico y la telefonía, con o sin soporte de Internet.

Organización para la Cooperación y Desarrollo Económico , creada en 1961, con sede actual en París, Francia y conformada por 30 países.

[25] ORGANIZACIÓN DE LAS NACIONES UNIDAS (O.N.U.), COMISION DE LAS NACIONES UNIDAS PARA EL DERECHO MERCANTIL INTERNACIONAL, “Origen, Mandato y composición de la CNUDMI”, Abril 2009
http://www.uncitral.org

Sus principales objetivos son propiciar el crecimiento económico sustentable, impulsar el empleo, elevar los niveles de vida de la población, mantener la estabilidad financiera, otorgar asistencia para el desarrollo de otros países, contribuir al crecimiento del comercio internacional.[26]

Dentro de Internet examina el impacto del comercio electrónico, en ramás como pago de contribuciones, fraudes, derecho del consumidor, seguridad.

Como se puede apreciar las cuestiones que se impulsan se dirigen sobretodo a los tópicos mercantiles para el caso de la participación gubernamental, y con excepción de la Unión Internacional de Telecomunicaciones, cuyo esfuerzo por soportar la Cumbre Mundial de la Sociedad de la Información es muy importante, hasta el momento se carece de principios e inclusive definiciones legales al respecto, uniformes para todos los países.

Es así que el trabajo de desentrañar al Internet toca a teóricos sociólogos, políticos, y expertos en información y comunicación, ingenieros en sistemas y computación, que en su mayoría forman parte de los sectores privado y social.

En el caso de nuestro país existe poca normatividad que se refiera al tema, entre ella:

Ley Federal de Telecomunicaciones[27], encargada de regular el uso y aprovechamiento de redes de telecomunicación, satélites y espectro radioeléctrico, entro otras, en este caso la conexión a Internet abarca el espacio de las redes de telecomunicaciones, aunque se deja de lado una referencia particular.

Reglamento Interno de la Comisión Federal de Telecomunicaciones[28], que establece, estructura y organiza este órgano que tiene a su cargo la aplicación de la regulación en materia de telecomunicaciones y promover su uso eficiente.

[26] ORGANIZACIÓN PARA LA COOPERACIÓN Y EL DESARROLLO ECONÓMICO "Marco Jurídico", Abril 2009 http://www.oecd.org
[27] Publicación D.O.F. 07-06-95. Inicio Vigencia 08-06-95, Ultima reforma publicada 09-02-09
[28] Publicación D.O.F. 02-01-06. Inicio Vigencia 05-01-06

Es importante señalar que en nuestro país ésta comisión es quien resuelve las interrogantes en materia de tecnologías de la información y comunicaciones.

Código Fiscal de la Federación[29]*,* en materia uso de redes informáticas estableció reformas publicadas en el Diario Oficial de la Federación el 5 de enero de 2004, que reglamenta cuestiones relativas al pago de contribuciones por medios electrónicos.

Código de Comercio[30]*,* en relación con la ley anterior, adiciona mediante reforma publicada en el Diario Oficial de la Federación el 29 de agosto de 2003, la Firma Electrónica Avanzada y el Certificado Electrónico, instrumentos de seguridad y certeza en transacciones comerciales en línea.

Código Penal Federal[31] , agrega mediante reforma publicada el 17 de mayo de 1999 el tipo Acceso Ilícito a Sistemas y Equipos de Informática en su artículo 211 bis , sancionado a quienes modifiquen, destruyan o provoque perdida de información, soportados en sistemas o equipos informáticos, en general computadoras y sus redes.

Nuevamente se da cuenta de la poca importancia que se da al hecho en estudio y sus posibilidades económicas, políticas, sociales y jurídicas.

La labor del jurista debe entonces dirigirse al estudio sistemático de este hecho que evoluciona a pasos gigantescos, sin pretender enmarcarlo en una ley local o reglamento que poco podría abarcar; centrando los esfuerzos en conceptualizar, establecer principios generales que se desenvuelvan junto al fenómeno y adecuen esta nueva realidad a la conducta humana.

[29] Publicación D.O.F. 31-12-81. Inicio Vigencia 01-01-83
[30] Publicación D.O.F. 15-09-1889. Inicio Vigencia 01-01-1890
[31] Publicación D.O.F. 14-08-31. Inicio Vigencia 17-09-31

1.3.5 Cumbre Mundial Sobre la Sociedad de la Información.

Es cierto que el Internet tiene capacidad de ubicarse casi en cualquier lugar del globo, y está por demás señalar los beneficios que trae para las sociedades que utilizan esta herramienta en las más variadas áreas.

Lamentablemente aún está lejos del alcance de cualquier persona en el mundo, ya que se trata como articulo de lujo, principalmente en países en vías de desarrollo, contrario a lo que sucede en los desarrollados que inclusive se equipara el acceso al sistema a un derecho humano, dentro del derecho a la información.

Esta diferencia se conoce como Brecha Digital o Tecnológica, que entendemos como:

La diferencia entre el desarrollo tecnológico de los países ricos en comparación con todos los demás, situación que ocasiona que los segundos estén obligados a importar tecnología a costos muy altos para mantener su competitividad y crecimiento, prolongando de manera indefinida su atraso.

En Ginebra, Suiza, del 10 al 12 de diciembre de 2003 y en Túnez, del 16 al 18 de noviembre de 2005, se realizó la Cumbre Mundial Sobre la Sociedad de la Información, auspiciada por la Organización de las Naciones Unidas y la Unión Internacional de Telecomunicaciones , siendo este el ejemplo más acabado de la sociedad internacional para lograr la reducción de la brecha tecnológica y alcanzar:

"El acceso universal, ubicuo, equitativo y asequible a la infraestructura y los servicios de las TIC…"[32]

[32] ORGANIZACIÓN DE LAS NACIONES UNIDAS (O.N.U.), UNION INTERNACIONAL DE TELECOMUNICACIONES, "Cumbre Mundial sobre la Sociedad de la Información", en CMSI Documentos Finales, Declaración de Principios de Ginebra, pág. 14 , Diciembre 2005 http://www.itu.int./wsis/index-es.thml

Esto es únicamente la unión del mundo en una conexión, a fin de lograr nivelar el crecimiento mundial y permitir de este modo una sociedad abierta a todo el planeta.

La Sociedad de la Información, es indefinida en los documentos resultantes, pero si menciona ciertos principios importantes, entre ellos, que está representada por una sola comunidad mundial, integrada por individuos libres con acceso ilimitado a las nuevas tecnologías de información y comunicaciones. Garantiza así mismo el acceso irrestricto a dichas tecnologías, reconociendo el acceso a la información y la comunicación como un derecho humano.

Para ello instrumenta diversos temas a desarrollar conjuntamente con los gobiernos, sociedad civil, organizaciones no gubernamentales, e individuos en particular, como protección de derechos de autor; estudios sobre gobierno del Internet; seguridad y privacidad de datos; privatización de la infraestructura de telecomunicaciones; promover la modernización del gobierno electrónico; promoción investigación y desarrollo, entre ellos se encuentran:

-*Gubernamentales.*- Organización de las Naciones Unidas, Unión Europea, Organización para la Cooperación y Desarrollo Económico, Grupo de los Ocho, Cooperación Económica Asia Pacífico, Organización Mundial de Comercio, Banco Mundial.

-*No Gubernamentales.*- Internet Corporation For Assigned Names and Numbers, Foro Económico Mundial, Global Business Dialogue and E-commerce, Global Information Infraestructure Commission (GIIC), Internet Society , Association For Progressive Communications.

Es importante señalar que el esfuerzo de la Organización de las Naciones Unidas por liderar un desarrollo y cooperación sustentable de las Tecnologías de la Información y la Comunicación es lento dado que se trata de integrar a todos los países del planeta, pero posee claros tintes sociales y humanísticos.

Es de lamentarse que la Global Information Infraestructure Commission en conjunto con diversos países y organismos internacionales, realiza negociaciones encaminadas a utilizar las Tecnologías de la Información y la Comunicación, principalmente el Internet, para explotar el comercio y marginar de este modo los derechos humanos, el desarrollo de los países pobres y el reconocimiento de un orden para estas tecnologías, por lo que es necesario limitar este tipo de esfuerzos en aras de proteger la equidad y la justicia dentro del sistema internacional.

En el caso de nuestro país, en el marco de la reducción de la brecha tecnológica el 02 de septiembre de 2010 se emitió el decreto por el cual se pretende dar el salto de la tecnología analógica a la digital mediante diversas acciones entre ellas la liberación de la frecuencia de 700 megahercios, apta para la prestación de os servicios de Internet, televisión por cable, telefonía móvil y fija; cuestión que en principio parece loable, más en la opinión de esta labor se cree que México aun es inexperto para dicha integración tan abrupta por lo que se cree que el móvil principal son motivos puramente económicos y políticos, más que de desarrollo social.

2. EL FENÓMENO JURÍDICO DE LA GUERRA Y SU CONEXIÓN CON EL INTERNET.

2.1 Definición y Naturaleza Jurídica de la Guerra

Es de vital importancia tomar en cuenta el alcance social que tiene la guerra, ya que el fenómeno forma parte de manera indisoluble de la historia y la naturaleza humanas, puesto que las revoluciones generan progreso.

La guerra puede tener el sentido de motor para la consolidación de Estados, tal y como lo afirma la Dra. Meza Salazar:

"Internamente la razón de Estado se identificación (sic) con la superioridad de los designios de la autoridad que inclusive puede hacer uso de la fuerza pública para lograr sus cometidos.
En el exterior se manifiesta para incrementar la potencia estatal, usando de todos los medios a su alcance, inclusive la guerra." [33]

En México existe una tradición pacifista, de neutralidad derivada de un siglo XIX muy turbulento, y por ende pocos aspectos de la guerra son estudiados por los juristas, sin embargo para el Derecho Internacional el fenómeno reviste capital importancia, sobre todo si se consideran los antecedentes del sistema internacional, que antes de la Segunda Guerra Mundial, imperaba en ellas el derecho de la fuerza, que operaba tal y como el mismo Maquiavelo señalaba a Lorenzo de Médicis en su obra El Príncipe:

"Un príncipe, pues, no debe tener otro objeto, ni cultivar otro arte más que la guerra, el orden y la disciplina de los ejércitos, porque este es el único arte que se espera ver ejercido por el que manda"[34]

Ya con posterioridad y con el surgimiento de la Organización del Naciones Unidas, así como la regulación del uso de la fuerza, sus efectos se ciñeron a un orden internacional, que si bien aplica a favor de unos pocos, a permitido periodos de estabilidad principalmente en el mundo occidental.

---

[33] MEZA SALAZAR, Martha Alicia, "Estado Telemático y Teoría del Estado", *Op. Cit*. Pág. 41
[34] MAQUIAVELO, Nicolás, "El Príncipe", Grupo Editorial Multimedios, México 1999, Pág 71

Una primera definición de Guerra Internacional es la siguiente:

"Es la que tiene lugar entre dos o más Estados y en la que se aplica el derecho de guerra consuetudinario y convencional, independientemente de que exista o no declaración de Guerra"[35]

La noción es corta al proporcionar detalles del significado de guerra en si mismo y se limita a citar algunas características de la guerra internacional, pero es posible ahondar en la idea principal.

La guerra implica un acto de violencia, el uso o amenaza de la fuerza que busca que alguien se someta a una voluntad ajena, la definición clásica de la guerra es la siguiente:

"La guerra es un acto de violencia cuya finalidad es forzar al adversario a ejecutar nuestra voluntad"[36]

Como se puede apreciar, esta concreta definición, proporciona mayores elementos para comprender la guerra, *en primer lugar* es un acto ya que el elemento voluntad es un requisito *sine qua non,* y del mismo se desean las consecuencias derivadas; *en segundo*, dicha actividad consiste en el deseo de obligar por la fuerza; *en tercero*, la presencia de un adversario; y *cuarto*, la finalidad, que es la imposición de una voluntad.

El maestro Modesto Seara Vázquez establece que la guerra es una:

"… lucha armada entre Estados, destinada a imponer la voluntad de uno de los bandos en conflicto, y cuyo desencadenamiento provoca la aplicación del estatuto internacional que forma el conjunto de las leyes de guerra".[37]

---

[35] INSTITUTO DE INVESTIGACIONES JURÍDICAS, Enciclopedia Jurídica Latinoamericana , Tomo V, Rubinzal – Culzoni Editores, Argentina 2007, pag. 752

[36] VON CLAUSEWITZ citado por VERSTRYNGE ROJAS, Jorge, "Una Sociedad para la Guerra; (los Efectos de la Guerra e la Sociedad Industrial)", Centro de Investigaciones Sociológicas, Madrid 1979, pág. 403

[37] SEARA VÁZQUEZ , Modesto, "Derecho Internacional Público", Ed. Porrúa, México, 1974, pág. 303 citado por GÓMEZ LARA, Cipriano "Teoría General del Proceso", Ed. Oxford, 10ª Edición, México 2004, pág. 17

Este autor ubica a la guerra dentro del ámbito internacional al establecer que la misma se desarrolla entre Estados, mantiene el elemento de imposición de voluntad mediante la fuerza así como el uso de armas, y ciñe el fenómeno a la aplicación de leyes internacionales que regulan el conflicto.

Además cita dos expresiones muy recurridas en el derecho internacional, la fuerza y las armas, mismas que por el momento se explican en los siguientes términos: por arma entendemos todo aquel instrumento que se utiliza para infringir daño y la fuerza es un poder físico, la capacidad que tiene un ser para imponer su voluntad sobre otro.

Por nuestra parte podemos señalar que *la Guerra es el conflicto armado entre Estados soberanos e independientes que suprime el estado de paz y tiene por objeto la imposición de intereses.*

En cuanto a su naturaleza, la doctrina clásica ha señalado, que más que jurídica, la guerra es un acto político, que se presenta cuando se conjugan los elementos de poder y voluntad necesarios para tratar de someter a otro por medio de la fuerza, cuando la diplomacia y la amenaza son ineficaces, en otras palabras su naturaleza deriva de ser un modificador de la realidad social, una revolución por la vía de la agresión.

Esta teoría obedece de manera clara al modelo imperialista de Derecho Internacional, el cual se traduce en la concepción del uso de la fuerza como una política de Estado, y supedita el Derecho Internacional a ser una simple justificación y legitimación del uso de la misma.

Se ha debatido mucho si el Derecho puede explicar e inclusive subordinar a la guerra; se cree que existen muchas razones que lo comprueban, por ejemplo, los acciones bélicas dentro de los Estados se atajan dentro de un orden normativo interno y responden a cuestiones de interés nacional exclusivamente y en cuanto a la guerra Internacional existe un orden acordado por los mismos, que para efectos prácticos se ha denominado Derecho de los Conflictos Armados.

Además este acto implica el desarrollo de principios jurídicos internacionales que reiteran su naturaleza como el uso de la fuerza, la violencia, la legitimidad, la coexistencia pacífica, la justicia.

Diversos autores han señalado que implica la guerra para ellos, en el caso de Jean-Jacques Rousseau:

"La guerra no es, pues, una relación de hombre a hombre, sino una relación de Estado a Estado, en la que los particulares no son enemigos más que accidentalmente, no como hombres, ni siquiera como ciudadanos, sino como soldados… Al ser el fin de la guerra la destrucción del Estado enemigo, se tiene derecho a dar muerte a los defensores cuanto que tienen las armas en la mano; pero en cuanto las entregan y se rinden, al dejar de ser enemigos o instrumentos del enemigo, vuelven a ser simplemente hombres y ya no se tiene derecho sobre sus vidas."[38]

Rousseau sostiene que la guerra se da exclusivamente entre Estados, ya que los hombres de forma individual solo forman parte del conflicto de forma incidental, el Estado es el que busca la destrucción del enemigo en aras de sus propios intereses, los que lamentablemente están lejos de ser representativos de lo que el autor denomina voluntad general.

El maestro Eduardo García Maynez, establece al hablar de normas internacionales, que la guerra posee una naturaleza sancionadora:

"Las normas internacionales no carecen de sanción, como a menudo se afirma. Aún cuando técnicamente muy imperfectas, tales sanciones existen. Las represalias y la guerra puede ser jurídicamente consideradas como sanciones típicas del *ius gentium*."[39]

La sanción es reconocida como una consecuencia derivado del incumplimiento de un deber, así la inobservancia del respeto, tolerancia, coexistencia pacífica, la justicia que existen entre los Estados pueden en un momento determinado derivar en represalias de orden bélico.

[38] ROUSSEAU Jean-Jacques, "El Contrato Social", Ed. Distribuciones Mateos S. A. Madrid, España 1993, Pág. 55
[39] GARCÍA MÁYNEZ, Eduardo, "Introducción al estudio del Derecho", *Op. Cit*. Pág 146

Por otro lado, también puede entenderse a la guerra como una facultad, tal es el caso de la que se da en legítima defensa.

Esta implica el ejercicio de un derecho, una facultad que se confronta a un hecho antijurídico, el uso de la fuerza esta encaminado a la defensa de un derecho, el sujeto responde a un peligro para evitarse un daño, sin importar la consecuencia.[40]

Para los procesalistas, existe un término que puede encuadrar la esencia de la guerra, el litigio, para Francesco Carnelutti es :

"el conflicto de intereses calificado por la pretensión de uno de los interesados y la resistencia del otro".[41]

La guerra posee particularidades que la distinguen del término anterior, basta con señalar que el litigio debe ser *jurídicamente calificado,* es decir que debe tener tal trascendencia que el Derecho otorga su tutela operando a favor de un interés, además de ser sometido a un juzgador que decidirá quien tiene razón.

La guerra carece de tutela, de un régimen especial que vele por ella, esto en virtud de que implica un acto irracional y antijurídico, por ello existen métodos pacíficos de solución de controversias; además la comunidad internacional carece de un órgano internacional con la capacidad de resolver cuestiones bélicas, en todo caso, los conflictos bélicos encuadran dentro de los medios de solución para estos conflictos de interés.

Entonces este fenómeno implica una forma de *autotutela* o *autodefensa*:

" La autotutela o autodefensa consiste en la imposición de la pretensión propia en perjuicio del interés ajeno".[42]

---

[40] GARCÍA MÁYNEZ, Eduardo, "Introducción al estudio del Derecho", Pág 227

[41] CARNELUTTI, Francesco, "Sistema de derecho Procesal civil", Trad. Niceto Alcalá Zamora y Castillo y Santiago Sentís Melendo, Buenos Aires, UTEHA, 1944, T. I pág. 44 citado por OVALLE FAVELA, José, "Teoría General del Proceso", Ed. Oxford, Cuarta Edición, México, 1998, pág. 5

[42] *Ibidem*, pág. 9

La pretensión es entendida por el maestro Cipriano Gómez Lara como la voluntad o intención exteriorizada, es decir manifiesta, de someter un interés propio al ajeno.[43]

Entonces la auto tutela es la exigencia de una voluntad exterior que nos obliga a someternos a su arbitrio.

Para Alcalá-Zamora y Castillo, existen distintos tipos de Autotutela permitida o tolerada, entre ellos, la legitima defensa, el ejercicio personal y directo de un derecho, el ejercicio de una potestad entre sujetos en litigio, así como el combate entre partes enfrentadas, que optan por el uso de la fuerza para la resolución de sus diferencias. En este ultimo tipo ubica al duelo y la guerra.[44]

Actualmente la guerra es inaceptable como medio de solución de conflictos, por tal razón, la misma se considera ilegal y solo es tolerada como medio para la legítima defensa ya que va más allá de el control de un Estado.

El maestro Gómez Lara nos señala al respecto que la Guerra es una forma autotulelar, colectiva, que enfrenta a sistemas distintos, y que rebasa el orden normativo de el Estado, derivado de el enfrentamiento de dos sistemas jurídicos nacionales.[45]

Del análisis anterior podemos afirmar de forma concreta que la naturaleza jurídica de la guerra implica una forma de autotutela, porque el sujeto que opta por esta decide utilizar la fuerza para someter un interés ajeno al propio, Colectiva ya que necesariamente participa un Estado en contra de otro como fuerza agrupada, antijurídica pues es contraria a los fines del derecho internacional, y relevante para el Derecho y las relaciones internacionales puesto que sigue presente y de forma constante produciendo consecuencias diversas, tolerada en casos concretos y bajo cierta vigilancia, conformándose un acto jurídico sujeto de forma incipiente a un orden normativo internacional, que busca encauzarlo, procurando así el menor daño posible.

:

[43] GÓMEZ LARA, Cipriano "Teoría General del Proceso", Ed. Oxford, 10ª Edición, México 2004, pág. 3
[44] ALCALA-ZAMORA Y CASTILLO, Niceto, "Proceso Autocomposición y autodefensa", UNAM, México, 1970, pp. 59-60 citado por OVALLE FAVELA, José, "Teoria General del Proceso", *Op. Cit*. pp. 13-14
[45] GÓMEZ LARA, Cipriano "Teoría General del Proceso", *Op. Cit*. pág. 18

2.1.1 Ius Ad Bellum y Ius in Bello

Es importante para efectos de esta investigación, conocer como se divide tradicionalmente la doctrina de guerra.

Ius Ad Bellum o Derecho a la Guerra, se refiere a las justificaciones de los Estados para recurrir a ella, son las razones, su finalidad es determinar que sujeto esta cometiendo una agresión y cuál la recibe, la principal justificante la encontramos en la legitima defensa que debe obedecer a diversos criterios señalados en la Carta de las Naciones Unidas.

Ius In Bello o Derecho de Guerra, se encarga del estudio del desarrollo bélico, los medios utilizados, y sus objetivos. Dentro de este podemos encuadrar las convenciones internacionales respecto de la guerra, por tierra, mar y aire, así como el uso y prohibición de cierto tipo de tácticas y armas, esta rama define los limites de lo que puede considerarse una conducta "aceptable" durante la guerra, principalmente se limita por los derechos humanos

2.1.2 Características Principales de la Guerra Convencional

Como particulares de la guerra podemos citar varias características:

-La finalidad militar siempre es la victoria, la imposición de la voluntad sobre el otro, en la doctrina antigua, se recurría a la *Guerra Absoluta*, la destrucción total del adversario, actualmente se pretende eliminar la capacidad ofensiva del mismo, el propósito así es la sumisión del enemigo.

-Los objetivos eternos de la guerra son: la supervivencia y seguridad del Estado como unidad política; el poder, entendido como la capacidad para influir en otros; y la gloria, es decir el reconocimiento de los demás Estados.[46]

[46] AARON, Raymond, "Paz y Guerra entre las Naciones", Ed. Revista de Occidente, 2ª Edición, Madrid, España, 1963, Págs. 101-126

-El tipo del conflicto bélico deriva del tipo de armas empleadas, antes se determinaba por el volumen de fuerzas y la logística. El volumen ya no tiene importancia y se utilizan sofisticados modelos de estrategia y análisis costo beneficio.

-En la doctrina clásica de la Guerra se reconocen cuatro elementos necesarios para que el deseo de imponer una voluntad sobre otro, se cristalice en el fenómeno bélico; espacio; material disponible y conocimientos; hombres y capacidad de adiestramiento; capacidad de acción colectiva tanto de el ejercito como de los ciudadanos.[47]

-El espacio o terreno donde se desarrolla la beligerancia está limitado al cielo, el mar o la tierra, aunque las grandes potencias se han preparado para enfrentamientos que utilicen como terreno el espacio exterior.

-Las causas de la guerra son muchas y variadas, pero de manera definitiva, la causa general de actividad bélica siempre deriva de desequilibrios en las relaciones de poder de los Estados, ya sean sociales, económicas, políticas, jurídicas, etcétera.
Esta inestabilidad puede concluir en agresiones y ataques armados, principalmente cuando se trata de problemas sociales o de población y económicos o de recursos.

-Existen distintos tipos de guerras, Infraestatales y se dan al interior de un Estado soberano, también conocidas como guerras civiles o revoluciones; Interesatatales, que enfrentan a unidades jurídico – políticas que se reconocen soberanía de manera recíproca; e Imperiales, que se dan a raíz del nacimiento de un Estado hegemónico que busca la consolidación de un bloque. Para efectos del presente trabajo todas son de interés, cada una a su debido nivel, pero únicamente las dos últimás poseen carácter internacional

-El inicio de las hostilidades puede darse de tres formás distintas; Declaración de Guerra, que implica una manifestación unilateral de voluntad del Estado

[47] AARON, Raymond, "Paz y Guerra entre las Naciones, *Op. Cit.* págs. 78-85

agresor; Inicio Efectivo; Ultimátum o Declaración de Guerra Condicionada, implica que el inicio queda sujeto a la realización de un evento determinado.

-En cuanto a los sujetos que intervienen, se pueden clasificar en dos tipos generales:

Beligerantes: son aquellos que efectivamente se encuentran en Estado de Guerra, y por ende asumen los efectos de la misma, mantienen el estatus de enemigos entre ellos mismos. Desde el punto de vista del inicio de la conflagración se encuentran también los Estados Agresores y Ofendidos.

Es muy difícil saber quien es el Estado que provoca el inicio de la guerra, el moderno Derecho Internacional, ha establecido que estos serán aquellos que abran efectivamente el conflicto, ya que la Carta de Naciones Unidas y sus principios básicos reconocen la acción bélica como antijurídica.

Desde la perspectiva de la forma de participación o rol, existen Combatientes y No Combatientes, que no son participantes efectivamente, sino un estatus que adquiere por defecto al inicio de la guerra, el no combatiente, será toda persona que se ve inmersa en el trance, pero no pelea en defensa propia ni ataca al enemigo, no pueden ser atacados, dentro de estos se menciona a la población civil general, cuerpos de paz, etcétera. Los Combatientes, representan una forma de participación activa en el conflicto, están legitimados para atacar y pueden ser agredidos en cualquier momento, entre ellos, los ejércitos profesionales.

Neutrales: Estados que han declarado su intención de mantenerse al margen del conflicto, su calidad produce efectos Erga Omnes.

-Terminación de las hostilidades, se da en tres formas distintas; Rendición, alguno de los Estados decide terminar el conflicto reconociendo la superioridad y sometiéndose a los intereses del otro; Conquista, el Estado ganador vence al enemigo y lo obliga al cumplimiento de sus demandas; Mutuo Acuerdo, que obedece al Principio de Polaridad, es decir, aún iniciado el conflicto deben

existir interlocutores de cada parte a fin de que las hostilidades sean limitadas y logre un acuerdo en cualquier momento.

Estos tipos dan lugar a la firma de tratados de paz, en los primeros se evita la negociación , ya que se obliga al vencido a aceptar las condiciones impuestas.

-Los Efectos de la Guerra son incontables, por lo que solo se citan de entre los más importantes: incremento de la mortalidad, carencia de recursos, beneficios o problemas económicos, integración o desintegración de Estados, concentración de poder, avance de la ciencia y la tecnología, aumento de crimen.

2.1.3 Regulación en el Derecho Internacional

Dado que la guerra es un acto evitado por los Estados en su mayoría, debido a sus efectos, la Carta de las Naciones Unidas en su articulo 51 establece que ninguna disposición prohíbe el Derecho de los Estados a la legitima defensa, es decir a repeler un ataque cuando es agredido por otro Estado, esto hasta en tanto la misma Organización tome cartas en el asunto.

En pocas palabras, la guerra en cualquiera de sus formas esta prohibida, únicamente se tolera cuando se actúa en legitima defensa de una agresión, comprendida esta última como:

"uso de la fuerza armada por un Estado contra la soberanía, la integridad territorial o la independencia política de otro Estado, o en cualquier otra forma incompatible con la Carta de las Naciones Unidas,…"[48]

La misma Carta establece la prohibición más amplia para el uso de la fuerza, en las relaciones internacionales, inclusive, el único facultado para recurrir a ella es el Consejo de Seguridad.

[48] ORGANIZACIÓN DE LAS NACIONES UNIDAS, Asamblea General, "Resolución 3314. Definición de la Agresión". Nueva York, Estados Unidos de América. Documentos Oficiales de la Asamblea General, Vigésimo Noveno Periodo de Sesiones. Suplemento No. 19. 2319ª Sesión Plenaria, 14 de diciembre 1974

Por lo que hace a la legitima defensa, opera a favor del Estado agredido, sin importar que el ataque cause daño o se haya consumado, aunque existen ciertas limitaciones a esta facultad reconocidas por la misma Carta en sus capítulos VI y VII.

Subsidiariedad. El estado agredido supedita su derecho al Consejo de Seguridad quien es el facultado para responder dicha acción violenta.

Provisionalidad. La defensa del Estado agredido debe prolongarse únicamente hasta que el Consejo de Seguridad tome las medidas pertinentes.

Deber de Informar. El Estado ofendido tiene la obligación de comunicar la agresión y las medidas adoptadas para repelerla.

Así mismo, la costumbre internacional estipula otros tantos:

Necesidad.- el estado agredido debe recurrir en ultima instancia a los medios armados.

Proporcionalidad. La legitima defensa debe ser desplegada de forma que exista una relación sensata entre el ataque y la respuesta.

Inmediatez. Se ejerce hasta la consumación del ataque armado.[49]

El limite de la defensa será la reciprocidad con el enemigo y únicamente dentro del tiempo que el Consejo de Seguridad de la Organización de las Naciones Unidas resuelva el asunto. Toda conflagración que inicie sin estos requisitos se entenderá como guerra de agresión y por ende, sujeta a sanciones y responsabilidad internacional por agresión, termino que deriva de el uso de la fuerza, ya que el Estado agresor es en si mismo un violador de la legalidad sin importar que resultado arroje el conflicto bélico, por ende esta sujeto a responder por la violaciones mínimas a derechos humanos, así como daños colaterales consecuencia de su incursión.

[49] CANO GARZON, Octavio Augusto, "La Doctrina Bush de la Guerra Preventiva. ¿Evolución del Ius Ad Bellum o vuelta al medioevo?". Ed. Universidad Pontifica Bolivariana, Medellín , Colombia, Vol. 36, No. 105. Julio – Diciembre 2006, págs. 399-428

De igual forma encontramos diversas disposiciones de carácter internacional que forman parte del *Ius in Bello*, ya que los organismos Internacionales han dejado de lado la cuestión teórica de la guerra y su conceptualización, así como la de sus componentes, en virtud de que se evita reconocerla como un medio de coerción, entre las más importantes existen:

Convención para la Adaptación de los Principios de la Convención de Ginebra, del 22 de agosto de 1864, a la Guerra Marítima , celebrado en La Haya, Países Bajos el 29 de julio de 1899, ratificado por México el 17 de abril de 1901, publicado en el diario Oficial de la Federación el 14 de septiembre de 1901, entro en vigor para nuestro país el 26 de enero de 1910.

Convención relativa al Rompimiento de Hostilidades celebrada en La Haya el 18 de octubre de 1907, firmada el mismo día, ratificada por el país el 29 de noviembre de 1909, entrada en vigor el 26 de enero de 1910 y publicada en el Diario Oficial de la Federación el 1 y 2 de febrero de 1910

Convención Concerniente a las Leyes y Usos de la Guerra Terrestre, celebrada el 18 de octubre de 1907, firmada el mismo día, ratificada por el país el 29 de noviembre de 1909, entrada en vigor el 26 de enero de 1910 y publicada en el Diario Oficial de la Federación del 3 al 10 de febrero de 1910

Pacto Briand – Kellog.- firmado en París el 27 de agosto de 1928, celebrado entre los países de Alemania, Estados Unidos de América, Bélgica, Francia, Gran Bretaña, Italia, Japón, Polonia y Checoslovaquia; a manera de antecedente, es el primer intento de la comunidad internacional por proscribir el uso de la fuerza en las relaciones internacionales y la búsqueda de medios pacíficos para la solución de controversias, el mismo tuvo pocos efectos, aunque sus postulados fueron recogidos por la Carta de Naciones Unidas.

Carta de la Organización de las Naciones Unidas, otorgada en San Francisco, Estados Unidos el 26 de Junio de 1945, ratificada por México el 7 de

noviembre del mismo año, y publicada en el Diario Oficial de la Federación el 17 de Octubre de 1945;

Convención de Ginebra de 12 de agosto 1949, que comprende 4 convenios todos firmado por México el 8 de diciembre de 1949, ratificado el 29 de octubre de 1952, entrando en vigor el 29 de abril de 1953 , publicado en el Diario Oficial de la Federación el 23 de junio de 1953

Convenio de Ginebra para Mejorar la Suerte de los Heridos y Enfermos de las Fuerzas Armadas en Campaña,.
Convenio de Ginebra para Mejorar la Suerte de los Heridos, Enfermos y de los Náufragos de las Fuerzas Armadas en el Mar
Convenio de Ginebra relativo al Trato de los Prisioneros de Guerra;
Convenio de Ginebra relativo a la Protección de Personas Civiles en Tiempo de Guerra

Su antecedente son tres convenciones anteriores celebradas en el mismo lugar durante los años 1864, 1906 y 1929

Convención Sobre la Protección de los Bienes culturales en Caso de Conflicto Armado.- celebrado en La Haya, el 14 de mayo de 1954, entro en vigor a partir del 07 de agosto de 1956 con el fin de regular las medidas de Derecho uniforme tendientes a la salvaguarda de los bienes culturales durante la guerra. Consta de 105 Estados parte al 26 de marzo de 2003. Ratificada por nuestro país el 07 de mayo de 1956 , publicada en el Diario Oficial de la Federación el 3 de agosto de 1956

Resolución No. 2131 Declaración de la Asamblea General de la Organización de las Naciones Unidas sobre la Inadmisibilidad de la Intervención en los Asuntos Internos de los estados y Protección de su Independencia y Soberanía, efectuada el 21 de diciembre de 1965, reconoce la libertad absoluta de los pueblos de la tierra, el respeto irrestricto a su soberanía, reafirma el principio de no intervención, establece como sinónimo de agresión a la

intervención armada, enfatizando que cualquier tipo de intervención sea armada o no, es una agresión, misma que pone en peligro la paz internacional.

Resolución 2625 Declaración de la Asamblea General de la Organización de las Naciones Unidas sobre los Principios de Derecho Internacional referentes a las Relaciones de Amistad y a la Cooperación entre los Estados de conformidad con la Carta de las Naciones Unidas; de 24 de octubre de 1970 se recapitulan los Principios establecidos en la Carta Original de 1945 y se reconocen la abstención a la amenaza o al uso de la fuerza contra el territorio o independencia política de cualquier Estado donde establece el termino de *Guerra de Agresión*; el arreglo de controversias por medios pacíficos recordando la igualdad soberana de los Estados; la no intervención en asuntos internos de los Estados; principio de cooperación obligatoria para el mantenimiento de la paz y seguridad internacionales; libre autodeterminación de los pueblos.

Resolución No. 42/22 Declaración de la Asamblea General de la Organización de las Naciones Unidas sobre el Mejoramiento de la Eficacia del Principio de la Abstención de la Amenaza o de la Utilización de la Fuerza en las Relaciones Internacionales, realizada el 18 de noviembre de 1987, donde se reconocen diversos principios como la cooperación internacional, la libre autodeterminación de los pueblos; responsabilidad internacional, para todo Estado que contravenga con lo establecido en dicha declaración.

Resolución No. 3314 Declaración de la Asamblea General de la Organización de las Naciones Unidas sobre la Definición de Agresión, de 14 de diciembre de 1974*;* señala como agresión el uso de las fuerzas armadas de un Estado cuando sean realizadas en contra de la soberanía, territorio o independencia política de otro, sea o no el Estado miembro de Naciones Unidas, asimismo enumera ciertos casos que se reconocen como agresiones sin limitarse a ellos.

Resolución No. 34/88 Declaración de la Asamblea General de la Organización de las Naciones Unidas sobre la Cooperación Internacional para el Desarme, adoptada el 11 de diciembre de 1979; en la cual se busca la reducción de el

armamento de los Estados derivado de la guerra fría, así como el exhorto a las naciones para evitar en todo lo posible el peligro de una guerra nuclear, la celebración de tratados al respecto y el uso de esos excedentes económicos en áreas de desarrollo social.

Resolución No. 37/10 Declaración de Manila sobre el Arreglo Pacífico de Controversias Internacionales, de 15 de noviembre de 1982, para evitar las acciones militares y hostilidades entre Estados, procurando acuerdos de buena fe sustentados en los principios de igualdad de los Estados y la libre autodeterminación de los pueblos, y someter a consideración de los mismos el reconocimiento de jurisdicción a la Corte Internacional de Justicia en los tratados que celebren.

Como se puede apreciar en su mayoría se realizan convenciones o resoluciones respecto de los medios por los que se hace la guerra y el como lograr la disminución de sus efectos tanto en las personas como en los bienes, objetivo principal del Derecho Humanitario o Derecho de los Conflictos Armados.

2.2 ¿Es posible la Guerra en Internet?

Definitivamente es posible la conducción de acciones bélicas dentro de las redes que conforman el Internet, ya que existen un sinfín de métodos o medios que permitirían y han permitido incursiones agresivas en contra de sistemas de Estados determinados, actualmente, estas hostilidades se limitan a simples ingresos a sitios para eliminar o modificar elementos, destruir información, inclusive inhabilitación de sistemas, pero se tiene planeado en un futuro próximo, atacar infraestructura estratégica.

Cada vez es más importante el número de ejércitos en el mundo que mantienen áreas especificas de sus cuerpos dedicados al desarrollo de la guerra cibernética, tal es el caso de Rusia, China y los Estados Unidos, inclusive en América Latina, Cuba, Venezuela, y Brasil mantienen un sigiloso pero constante desarrollo de este brazo bélico. Hasta la década pasada era

risible la posibilidad real un enfrentamiento en el ciberespacio, pero el avance inusitado de las tecnologías de la comunicación y las comunicaciones permiten dichos choques.

Cada vez que se presenta uno, los ejércitos del mundo y los expertos indagan en su realización, causas, medios, recursos y efectos, estudiando un fenómeno que es y será para el futuro una nueva forma de hacer la guerra.

2.2.1 Internet como Campo de Desarrollo de Conflictos Bélicos entre Estados.

¿Cómo entonces puede ser Internet, campo de batalla principal de un conflicto armado?

De principio se debe recordar que este espacio, es parte de nuestra vida cotidiana, y cada sistema de tecnología moderna puede ser en cualquier momento apto para conformar uno de los tantos nodos o terminales que engrosan día a día la Internet, desde los servidores de acceso, computadores personales, teléfonos y dispositivos móviles, dispositivos de identificación biométricos, por solo citar algunos

Desde el punto de vista jurídico, los obstáculos para que sea considerado como un nuevo territorio objeto de conflagraciones, son casi nulas, muchos Estados tienen en sus divisiones militares áreas especificas de expertos en informática y cibernética, que desarrollan armas para diezmar las fuerzas enemigas.

Por otro lado, estos expertos se han enfrentado en más de una ocasión dentro de dicho espacio, tratando de sabotear tanto simples páginas de Internet, como sistemas estratégicos, de defensa, telecomunicaciones, finanzas; se suprime el estado de paz que imperaba con anterioridad en el momento que se detecta este tipo de actividades dentro de la red.

Muchos Estados utilizan este recurso en coordinación con intervenciones típicas; por último, su objetivo deja a un lado la destrucción del enemigo, limitar

sus recursos o matar a la población, su finalidad es ejercer coacción con el fin de lograr el sometimiento del enemigo a intereses determinados.

2.2.2 Sistemas de Control Informático

Esta frase hace referencia a los medios, técnicas o procedimientos que son utilizados para el mejor manejo de Información; en este caso mencionaremos solo algunos que a lo largo del siglo XX permitieron el surgimiento y avance de redes tan amplias como Internet, el objetivo es observar como el desarrollo de la tecnología permite el control y gobierno de actividades tan cotidianas como las redes informáticas, de manera tal que ese espacio virtual, prácticamente es una dimensión paralela a nuestro mundo, y que para efectos del presente trabajo implica un nuevo campo de batalla para intervenciones bélicas.

-Máquina de Turing.- creada por el inglés Alan Turing, padre de la inteligencia artificial, es el primer modelo de cálculo que aparece en la historia, siguiendo algunas reglas especificas y preestablecidas, solo requiere de algunos datos iniciales para realizar operaciones, obteniendo resultados en un tiempo específico.

-Enigma.- maquina desarrollada durante la segunda guerra mundial, al servicio de la fuerza aérea y armada alemanas, consistía en un dispositivo que se conectaba a las máquinas de teletipo que utilizaban el código Morse para codificarlo.

-Colossus.- primer computadora electrónica del mundo diseñada en Inglaterra durante la segunda guerra mundial, a fin de descifrar los mensajes secretos de la milicia Alemana.

-Echelon.- sistema informático compuesto de superordenadores, capaz de interceptar diariamente el 90% de las comunicaciones de la red, incluyendo, llamadas telefónicas, mensajes de correo, descargas de Internet, transmisiones vía satélite, etc. Contiene datos específicos, nombres, direcciones, teléfonos,

números de tarjetas, contraseñas. Forma parte de un esfuerzo conjunto de las agencias de inteligencia estadounidense y europeas, a fin de espiar estas telecomunicaciones y sondear el flujo de información en Internet.

En la actualidad este sistema sigue en funcionamiento, activistas de decenas de países tratan de organizarse para eliminar lo que señalan como la amenaza más grande a la intimidad de las personas en el mundo.

Estos sistemas, son la antesala de los mismos que vigilan y protegen las fronteras cibernéticas de cada país, constituyen la protección de información de las infraestructuras críticas de los Estados.

2.2.3 Guerra Informática

La importancia de conocer la Guerra Cibernética como nuevo medio para las hostilidades en materia internacional es bastante difusa si se deja de lado su componente más importante, la guerra informática, como se apreciara en el tercer capitulo, son cosas distintas, por lo que es imperativo conocerlas de forma separada.

Ésta clase se basa en las debilidades de los sistemas y redes del enemigo y su arma comprende programas informáticos y ordenadores, su objetivo será afectar al enemigo de tal forma que sus procesos de información se entorpezcan o se inutilicen.

La Guerra Informática se define como:

"Acciones dirigidas a lograr la superioridad en la información, atacando la información, los procesos informáticos, los sistemas de información y las redes computarizadas del enemigo a la vez que se defienden la información, los procesos informáticos, los sistemas de información y las redes computarizadas propias". [50]

[50] ADAM, James , La Próxima Guerra Mundial, Ediciones Granica, México 1999, pag. 82

La guerra informática es un conflicto cuya particularidad estriba en los objetivos de los ataques, en este caso, la meta es reducir, eliminar o manipular la información que el enemigo maneja con la finalidad de entorpecer su funcionamiento, buscando el error en sus operaciones e inclusive su parálisis parcial o total, sería muy aventurado decir que se limita al uso de ordenadores, cuando en realidad cualquier actividad que cause daño e la información que el enemigo utiliza para su toma de decisiones, forma parte de este tipo de guerra.

Se aprecia que efectivamente existen los elementos necesarios para considerar este tipo de acciones como agresiones directas, que serán sujetas del Derecho Internacional cuando las mismas rebasen las fronteras locales o implique a más Estados.

2.2.3.1 Tipos

Entre los tipos más frecuentes de guerra informática podemos encontrar los siguientes:

-Guerra Antipersonal.- se constituye por ataques contra la intimidad y los datos personales; lo que implica la revelación, alteración o destrucción de los mismos. Un ejemplo se tiene en las bases de datos de las diversas dependencias de gobierno, que inclusive venden información a sectores privados para cuestiones de marketing o publicidad; un intruso en estas bases puede alterar nuestra información personal, pudiendo en teoría desaparecer o crear personas jurídicamente, por ejemplo, en México existe actualmente el debate respecto de la llamada Cedula de Identidad Ciudadana y los datos que el gobierno desea concentrar en una base, mismos que parecen extremos e inclusive violatorios de la intimidad.

-Guerra Corporativa.- se da entre sectores privados, principalmente comerciales e industriales quienes recurren a expertos en la penetración de sistemas a fin de robar información clasificada, como investigaciones, desarrollos de nuevos productos. Gran parte de este tipo de invasión obedece

al remanente de espías que al fin de la guerra fría buscaron en el sector privado un medio de sobre vivencia.

-Guerra Global.- se aplica principalmente en sujetos de Derecho Internacional, Estados o empresas transnacionales, quienes mediante este tipo buscan la destrucción de los sistemas enemigos. Desafortunadamente la distancia física pasa a segundo plano y las medidas preventivas están lejos de proporcionar seguridad absoluta, por lo que con una inversión baja, países en desarrollo o inclusive terroristas podrían destruir en teoría el sistema financiero de un país, provocando perdidas incalculables y pánico mundial.

2.2.3.2 Recursos

Dentro de las "armas" que utiliza la guerra informática, para la consecución de sus fines encontramos:

-Virus Informático.- programa dañino, autorreproducible y subrepticio, cuyo objetivo de acuerdo a su tipo es autocopiarse tantas veces como pueda con el fin de alterar la capacidad de un sistema para trabajar, en cuyo caso es conocido como g*usano ,* o la introducción de sentencias en la estructura de un programa para permitir la ejecución de otro no autorizado, y es llamado c*aballo de Troya.* Sus efectos son generalizados para todo sistema con el que tenga contacto.

-Bombas Lógicas.- programa ejecutado en un momento especifico al cumplirse determinadas circunstancias. Un ejemplo, sería una orden codificada para que determinados componentes de un ordenador exploten.

-Puertas Traseras.- interrupción de la lógica de un programa en la fase de desarrollo para su depuración y uso con fines delictivos. Una empresa fabricante de software, crea un programa que permite a la misma empresa extraer datos de cualquier ordenador donde se instale.

-Ataques Ping.- solicitudes de servicio de acceso que se multiplican por cientos y miles saturando servidores, ancho de banda y dejando inservibles servicios y paginas cibernéticas.

-Armas Digitales.- el ultimo eslabón en al desarrollo de medidas para el acceso y destrucción de sistemas informáticos.

Es un programa informático elaborado profesionalmente con el fin de producir un daño específicamente dirigido. Asimismo el programa incluye contramedidas ante recursos de defensa pasiva, activa o automática. Cuentan con complementos digitales que refuerzan su defensa y ataque, estos instrumentos poseen inteligencia propia, son armas dirigidas a un blanco con el fin de hacer daño, de una precisión y efectividad mayor que las de los recursos militares tradicionales.[51]

2.2.3.2 Objetivos

Los objetivos principales de este tipo de intervenciones en particular son muy variados, dentro de un conflicto bélico, se puede contaminar el flujo de información del enemigo; controlar el entorno Internet, con el fin de confundir, engañar o encubrir información, provocando daños al sector civil y militar; dañar la estructura logística del enemigo logrando la dispersión de las fuerzas enemigas; robar información estratégica confidencial; dañar los sistemas de abastecimiento de la población, entre otros.

2.2.4 Problemas actuales

De manera paralela al problema que implica este tipo de actividad bélica, existe acciones realizadas por civiles, utilizando los mismos medios de que se vale la guerra cibernética, con el fin de delinquir o infundir terror en los Estados o sistemas enemigos.

Con esto se comprende que la amplitud de estos movimientos alcanza cualquier nivel de la población mundial, entre los más comunes encontramos los siguientes.

[51] LOPEZ, Claudio C. *La Guerra Informática*, en Boletín del Centro Naval, S. E. , Argentina, número 817, Mayo – Agosto 2007, pags. 221-222

2.2.4.1 Ciberdelincuencia

La ciberdelincuencia implica actividades antijurídicas, encaminadas a la comisión de delitos mediante el uso de tecnologías informáticas. Entre las actividades más recurrentes se encuentran: falsificación de datos y documentos; vandalismo electrónico, es decir el ingreso sin autorización a sistemas cibernéticos sin el afán de dañar la estructura principal del mismo, pero con dejando marcas y daños menores, por ejemplo graffiti virtual; robo de datos; fraudes financieros; inundación de mensajes de supuesto origen desconocido (*spam*); extracción ilícita de información personal con fines publicitarios o de marketing (*phishing*); difusión de material ilícito y nocivo; uso no autorizado de programas computacionales; destrucción de programas; secuestro de soportes magnéticos; sabotaje político.

2.2.4.2 Ciberterrorismo

Únicamente como referencia, esta actividad, implica la comisión de actos en caminados a infundir miedo en determinados grupos sociales o Estados, mediante el uso de violencia, con el fin de lograr un cambio en la estructura económica, política, social, utilizando par tal fin las tecnologías de la información.

Es factible, dado su bajo costo y efectividad, el uso de la informática con fines de presión a favor de grupos terroristas y en contra de gobiernos nacionales.

Sus principales objetivos, son bancos, áreas de gobierno, centrales telefónicas, medios de comunicación, centrales eléctricas y nucleares.

3. GUERRA CIBERNÉTICA

3.1 Marco Conceptual

En el apartado anterior se analizó el concepto de guerra así como algunas de sus características e implicaciones jurídicas, a continuación se realiza un análisis de la cibernética, ciencia que da vida al fenómeno en estudio, la misma se define como:

"Estudio analítico del isoformismo de la estructura de las comunicaciones en los mecanismos, en los organismos, y las sociedades"[52]

El termino isoformismo es unicamente la identidad que existe entre dos sistemas.

La palabra Cibernética proviene del griego *ciber* que significa timonel o piloto,

Algunos autores sostienen que el término fue utilizado por primera vez en 1848 por el físico y filosofo francés Ampere, al clasificar las ciencias políticas.[53]

Su origen como ciencia se remonta a la segunda guerra mundial, en el trabajo estadístico desarrollado por el estadounidense Norbet Wiener, cuando se presento el problema del desarrollo de los denominados cerebros electrónicos y los mecanismos de control automático para los equipos militares como aquellos que se encargan del posicionamiento de los misiles y la ubicación de los objetivos.

El concepto conocido actualmente, fue aplicado por primera vez en 1948 en el libro CIBERNETICA: o Control y Comunicación en el Animal y la Máquina, del mismo autor.

[52] WIENER, Norbet, "Cibernética y Sociedad", S.E. 1954, Pág. 11 citado por LIVAS, Javier, "Cibernética, Estado y Derecho", Ed. Gernika, México 1988, Pág. 86
[53] *Ibidem*, Pág. 85

"Norbert Wiener fue el creador de la cibernética como ciencia de unidad multidisciplinaria que se aboca a la comunicación y control entre maquinas y seres humanos para abarcar de forma totalizadora a todas las ciencias."[54]

De la misma forma, Fernández Rodríguez nos señala:

"La *cibernética* es la ciencia de las máquinas dirigidas por programas en ellas incorporados u operativos en las mismas. De esta forma, se estudian las analogías entre los sistemas de control y comunicación de los seres vivos y de las máquinas, buscando aplicaciones de los mecanismos biológicos a las mismas" [55]

La cibernética se encarga de observar y analizar de igual forma los sistemas de comunicación y control de los organismos vivos, y los de las máquinas, la forma en la que captan los impulsos del ambiente y su respuesta, a fin de crear modelos similares de control, es importante señalar en este punto que la informática es una derivación de la cibernética como ciencia raíz, su objeto es la información, su uso y manejo automatizado, la cibernética va más allá y comprende la comunicación y el control de forma total.

Esta ciencia trata de seccionar un objeto, describiéndolo en si mismo y en su relación con los demás objetos de su alrededor, logrando mejorar sus conducta en concordancia con el ambiente que lo rodea, es decir que trata de mejorar la comunicación del objeto con el sistema y lograr el equilibrio del mismo.

Para entender lo anterior será necesario pensar en cualquier ente, vivo o maquina, este se organiza y responde a lo impulsos del ambiente con una determinada réplica, esta se graba en el sistema, proporcionando una cierta experiencia que servirá para cada caso futuro, dada la variabilidad del mundo, el cúmulo de información se vuelve infinita, al igual que las posibles respuestas, pero siempre obedecerán a un orden determinado, que se puede establecer mediante análisis y estadística.

[54] MEZA SALAZAR, Martha Alicia, "Estado Telemático y Teoría del Estado", *Op. Cit*. Pág. 100
[55] FERNÁNDEZ RODRÍGUEZ, José Julio, "Lo Público y lo Privado en Internet. Intimidad y libertad de expresión en la Red", *Op. Cit.* Pág. 2

Este principio se conoce como *feedback* (realimentación), que constituye el concepto fundamental de la automatización, o como lograr que una máquina responda ante su entorno de la misma forma que un ser vivo lo hace.

La cibernética estudia al hombre como sistema y su relación con el medio, así cada sistema esta diseñado para interactuar en forma determinada, esta ciencia proporciona modelos más efectivos para lograr una mejor correspondencia, basada en un control determinado, entendido como el mecanismo que corrige y equilibra el funcionamiento de los sistemas.

Para la cibernética, el Derecho como sistema de conducta humana no puede ser automatizado en si, es decir es impredecible, contrario a los modelos matemáticos, o cualquier fenómeno físico, su particularidad radica en que forma parte de los sistemas de control social, como lo son por ejemplo la moral, la religión.

El Derecho, a pesar de ser una ciencia, carece de “leyes”, entendidas como normas universales; con la cibernética, es posible medir las relaciones que trata de regular y establecer descripciones, estudiar cada institución, a fin de fundar principios generales, que permitan mejorar las relaciones de los individuos.

En un ejemplo, dentro del Derecho Internacional, la cibernética esta en posibilidades de estudiar el fenómeno de la guerra y su prevención; al verificar las causas y los fines, los sujetos involucrados y los medios utilizados; derivado de este análisis puede resolver que en las últimas décadas, las intervenciones militares responden a motivos puramente económicos y políticos para mantener la hegemonía de los Estados capitalistas desarrollados así como de empresas transnacionales, los medios están dirigidos al control de regiones mediante el mejor uso de información y armamentos más precisos, abaratando costos y mejorando la comunicación. Con este estudio se puede producir un modelo que señale las probables características futuras del fenómeno y de esta forma adelantar la celebración de Tratados que limiten este tipo de ofensivas, mejorando y ampliando el control del derecho sobre la acción humana.

Mediante la cibernética se puede lograr el estudio detallado del Derecho y generar mejores instituciones, leyes efectivas realmente, y en caso de ser necesario, realimentar al sistema con los resultados, de este modo perfeccionar las relaciones y la conducta.

3.2 Naturaleza Jurídica y Características Principales de la Guerra Cibernética

Con anterioridad se trató de desentrañar la naturaleza jurídica de la guerra convencional, se dijo que se trata de un medio de auto tutela, en el cual un Estado trata de imponer su voluntad a otro.

La guerra cibernética, como un nuevo tipo de conflicto, comparte la misma problemática que la guerra en general, de hecho, es únicamente un nuevo campo de batalla, inaceptado aún, al igual que lo fueron en su momento el aire y el espacio, la gran diferencia entre las guerras cinéticas y el guerra cibernética radica en los recursos, el personal y las armas. Las causas y motivos siguen siendo políticos, sociales y económicos. Difieren los efectos pero los fines son similares.

Jurídicamente implica un acto que busca imponer una voluntad sobre otra mediante el uso de mecanismos de control de comunicaciones e información; es un acto por las consecuencias, que necesariamente repercuten en la esfera del derecho; es antijurídico porque es inaceptable el uso de la fuerza para imponer una voluntad o ejercer presión; su particularidad estriba en el espacio donde se desarrolla y los recursos de los que echa mano.

Este fenómeno carece de regulación o explicaciones detalladas, uniformes, excepto por las generalidades que ya existen fijadas para el desarrollo de conflictos bélicos, al ser un tipo relativamente reciente, es por ello la necesidad de este análisis y descripción legal.

Para comprender mejor esta nueva situación, se establecen algunas características generales:

- Como fenómeno político social, económico y jurídico se mantiene estable y en concordancia con la guerra convencional de tipo cinético, las causas y fines son invariables.

-Su campo de desarrollo principal es el ciberespacio, sin estar restringido al mismo.

- La principal forma de comenzarla es mediante el inicio efectivo de hostilidades, ya que la sorpresa es necesaria para atacar sistemas enemigos.

- La guerra cibernética permite la compresión de la distancia y el tiempo de los conflictos.

-Se ejerce en dos vías, ofensiva y defensiva, los ataques tienden a desestabilizar los sistemas enemigos mientras la defensa evita que las conexiones abiertas por dichas embestidas queden sin protección, haciendo susceptible una represalia.

- Los recursos o armas de las que se vale son tecnologías avanzadas que se auxilian de la velocidad en que se obtiene, procesa y transmite la información.

- Estos mismos son muy accesibles, baratos y de alta interactividad, ya que los nuevos ordenadores son muchos más sencillos de manejar que los primeros existentes.

- El personal se conforman por especialistas en manejo de información y nuevas tecnologías.

- El número de combatientes es poco importante, ya que unos cuantos expertos pueden manejar muchísimas terminales de forma automática.

- Evita la confrontación directa, el choque de fuerza, se prefieren operaciones de inteligencia, captura, análisis y transmisión de información.

- Existe facilidad en el uso de mercenarios, dada la sencillez para mantener un cierto nivel de anonimato en el ciberespacio, los combatientes pueden ser tanto nacionales como civiles afines a cierta causa, que dada su cultura no obedecen nacionalidades y se sitúan en cualquier lugar del globo.

- Sus operaciones llevan el término de exactitud en el ataque a su máxima expresión, es decir, se establecen avanzadas más precisos, dirigidos principalmente a sistemas estratégicos y bases de datos.

- A pesar de la precisión de los ataques, el nivel posible de daño colateral, aumenta cuando se apunta a infraestructura crítica de los países.

- Su objetivo es someter al adversario sin disparar un solo tiro, mediante el mejor manejo de los flujos de información y comunicación, busca la desestabilización o neutralización de los sistemas de control que el enemigo posee.

- Previene el uso de tropas de campo, con lo que se reduce el número de bajas de combatientes.

3.3 El Problema de la aplicación del Derecho a la Guerra Cibernética

Para que el Derecho este en posibilidad de analizar un nuevo fenómeno de la realidad, es necesario en primer lugar que dicha situación repercuta en la esfera de los hombres, de las sociedades, y en segundo, la voluntad de los investigadores para analizar, de las escuelas y facultades para estudiarlo y la de los gobiernos para adecuarlo al orden normativo correspondiente.

En el caso de la guerra cibernética, la realidad de nuestro pensamiento aún limitado a la pura esfera jurídica, el desconocimiento y la velocidad de evolución de las nuevas tecnologías, así como su importancia en las relaciones y conducta humanas representan el primer obstáculo.

Otro límite para que el Derecho dirija su atención a esta nueva realidad es que el mundo desestima su capacidad, observan a lo de lejos su crecimiento, la amenaza de una guerra librada en el ciberespacio y los sistemas informáticos y de comunicaciones en general, es muy real, el Derecho se ha limitado al buscar respuestas adecuadas, ya que aún se piensa en amenazas de tiempo y espacio tangible.

El ciberespacio carece de una definición apropiada, la costumbre o la ley internacional poco han podido ante este fenómeno, así que se debe entender que este nuevo campo para el desarrollo de las actividades humanas también responde al uso con fines bélicos.

Además existe la falsa creencia de que el ciberespacio carece de un orden legal, pero contiene normas, códigos de conducta, e inclusive sanciones para quienes hacen mal uso del mismo, es importante atender a este tipo de autorregulación.

La falta de cooperación entre países, a pesar de la Cumbre Mundial de la Sociedad de la Información, es una realidad, el mundo nunca estuvo tan conectado entre sí y los Estados tan alejados.

Ante esto último es difícil establecer bases uniformes o principios generales cuando existe la brecha tecnológica. En el nivel local de cada Estado, existen ciertos avances en materia de regulación de cuestiones comerciales, valor probatorio de constancias derivadas de la red, autenticación de usuarios, pero estos son inaplicables a los países foráneos.

El sector privado trata de limitar la regulación estatal en todo aspecto, a fin de dominar cada vez más mediante el poder económico a los gobiernos; el ciberespacio también padece esta situación, ya que el uso de los medios de los que se vale la guerra cibernética están a la orden para el robo de secretos industriales, información clasificada y privilegiada, bases de datos gubernamentales.

Es necesario limitar ciertos actos de molestia tanto de los gobiernos y los particulares en cuanto a vigilancia y seguridad en Internet. Por ejemplo la vigilancia en exceso de parte de las policías cibernéticas, puede ser entendida como invasión a la intimidad; así estas cuestiones, relevantes para mantener un cierto orden en la libertad de los flujos de comunicación e información, se topa siempre con la barrera de los Derechos Humanos, que por ser personales están ligados al ser y deben mantener su reconocimiento así como ejercicio a pesar de que el territorio sea intangible.

El rastrear una acción hostil es sumamente difícil, pero posible, así que una respuesta o represalia tardía puede traer consecuencias de ilegalidad o ilegitimidad en la defensa.

En resumen, de estos problemas derivan cuestiones como: el tiempo, en cuanto a la velocidad del desarrollo del fenómeno; el espacio, la definición y delimitación del ciberespacio; los sujetos involucrados, Estados, civiles y corporaciones; ¿Quiénes serán los nuevos combatientes? ; jurisdicción, ¿ante quien se resolverán estos problemas?; adecuación o creación de nuevos principios, que expliquen la agresión, el uso de la fuerza, armas, daños; la seguridad y la vigilancia de los sistemas; la eliminación de la brecha tecnológica; el reconocimiento de nuevos derechos humanos inclusive.

Empero existen ya intentos que buscan desentrañar la trascendencia de las nuevas tecnologías y sus fines que de forma amplia se ha encaminado en un principio a la Teoría del Estado:

"El Estado Telemático pretende aprovechar todos los adelantos científicos para incrementar su poderío, pero sería terrible que por su mal empleo se desencadenara una tercera guerra mundial que ya no sería simplemente atómica sino algo más y acabaría con el mundo. Información digitalizada, telecomunicaciones y Revolución Informática son las características sobresalientes del Estado Cibernético que funda su poder en la información, a la cual puede socializar o monopolizar."[56]

[56] MEZA SALAZAR, Martha Alicia, "Estado Telemático y Teoría del Estado", O*p. Cit.*, Pág. 59

3.3.1 Delimitación y definición práctica.

La guerra del Golfo Pérsico desarrollada por una coalición de países liderada por Estados Unidos de América en contra de Irak, y cuyo fin principal era la retirada de las tropas iraquíes de los territorios de Kuwait; fue el último gran conflicto bélico de carácter convencional.

En el se exploraron por primera vez en campo las posibilidades de la guerra cibernética, ya que el éxito de gran parte de sus operaciones se deben al mejor tratamiento de la comunicación y la información, así como el uso de nuevas tecnologías.

La guerra cibernética mantiene relación con otros términos como la *guerra electrónica* que se vale de medios electrónicos para desestabilizar lo sistemas de control enemigos, afectado principalmente comunicaciones y funcionalidad de aparatos, así como la *guerra informática*, misma que se definió en el capitulo anterior; pero debemos entender que la Cibernética incluye la utilización de ambas, inclusive forman parte integral de su definición.

Por lo tanto, la guerra cibernética incluye el uso de todas las herramientas disponibles al nivel de electrónica e informática para eliminar los sistemas enemigos, sosteniendo los propios en niveles operacionales.

Por estas consideraciones se define la Guerra Cibernética como *el acto por medio del cual Estados soberanos en conflicto pretenden la imposición recíproca de intereses mediante el uso de herramientas electrónicas e informáticas, dirigidas a la supresión de los sistemas de control enemigos, al tiempo en que se sostienen los propios.*

La guerra cibernética implica mucho más que la guerra informática, esta ultima es una especie, ya que se limita a los sistemas de información, desde su obtención hasta su utilización, la informática esta aplicada por ejemplo en espiar, infiltrar sistemas y redes mediante computadoras; la guerra cibernética va más allá, busca la destrucción de los recursos del oponente, el control a

distancia de los medios propios, la planificación de operaciones, y cuestiones importantes de logística como el abastecimiento de las tropas, todo mediante el uso de tecnologías electrónicas, informáticas y de comunicación, teniendo como campo principal las redes mundiales.

Los recursos de los que hecha mano son tecnologías nuevas, avanzadas, que obedecen al mejoramiento del uso, flujo y tratamiento de la información, así como la inteligencia simulada; combina la informática, la dominación del ciberespacio, las micro y nano tecnologías, el uso de armas no letales, la robótica y las operaciones psicológicas para lograr el control de un sistema, de un Estado.

Es una realidad que existen poderes de hecho que en algún momento pueden hacer uso de los medios de la guerra cibernética, como grupos terroristas y las corporaciones comerciales. Pero jurídicamente se evitó contemplarlas dentro de la definición dado que son incompatibles con la naturaleza de los Estados en el plano internacional, es decir que, estas agrupaciones obedecen a un orden inferior, es facultad de cada Estado en particular regularlos, reconocer su capacidad de facto implicaría otorgarles el nivel de sujeto internacional, situación que es por demás polémica.

Lo cierto es que la amplitud de la guerra cibernética evita su estudio pormenorizado, es por ello que la presente labor esta limitada a los aspectos más importantes, como sus implicaciones en el ciberespacio.

3.3.2 Soberanía

La soberanía es el elemento jurídico que junto al gobierno (*elemento político*), el territorio (*elemento geográfico*) y la población (*elemento humano*) conforman el Estado, que para efectos de esta investigación interesa en cuanto a su carácter de sujeto del derecho internacional.

Las concepciones históricas de la soberanía se centran en que el sujeto que la detenta o el ente del cual emana, se reconoce siempre como potestad o

facultad, con la característica siempre presente de permanencia, poder absoluto unificado en un sujeto o un conjunto de sujetos para regir o decidir en un espacio y tiempo determinados.

En las concepciones antiguas, la soberanía se pensaba provenía de Dios y este transfería su potestad a los reyes, posteriormente se expreso que el Estado Moderno durante el siglo XVII era el soberano como ente unificador y organizador de la política, su modificación por la concepción francesa del poder del pueblo, hasta la teoría de el orden jurídico como soberano.

Para ampliar un poco esta concepción se cita el siguiente pensamiento:

"… el estado es soberano; esta formula significa que el estado es una unidad territorial decisoria universal y efectiva, tanto en su interior como hacia el exterior. La potencialidad universal de la decisión implica supremacía e independencia jurídicas. Decir que un estado es soberano significa que es una unidad decisoria universal dentro de su territorio."[57]

Se entiende la soberanía como el poder de una nación para otorgarse una determinada regulación y organización evitando factores externos, es indivisible, absoluta, otorga libertad interna y a nivel internacional la soberanía se encamina hacia el reconocimiento de independencia y forma parte un principio básico para la coexistencia pacífica.
Las naciones pueden auto determinarse en la forma que más convenga a sus intereses.

La soberanía es el concepto en que descansa la mayoría del sistema de relaciones internacionales, ya que la misma da legitimidad al Estado como ente representante de una nación, gracias a ella, los Estados se reconocen un nivel de igualdad, y se acepta que ninguno tiene autoridad sobre otro. El poder que pueden desplegar políticamente ya sea con el uso de la fuerza o mediante la diplomacia, varía enormemente en el plano mundial, ya que no tienen la misma envergadura que el poder interno del Estado , ni usa sus mismos métodos en el mismo espacio.

[57] HELLER, Hermann, "La Soberanía", Ed. UNAM y Fondo de Cultura Económica, 2ª Edición, México 1995, Pág. 225

Es necesario el estudio de este concepto dado que una de las posibilidades que otorga la soberanía es el uso de la guerra como potestad del Estado para defenderse; es por ello que este pensamiento posee dos vertientes importantes en el estudio de la guerra cibernética.

La primera descansa sobre la posibilidad de que un Estado regule las interacciones que se dan en un espacio global común, el ciberespacio; es un problema saber si la soberanía estatal abarca las redes y sistemas informáticos, además de que el Estado carece de poder para determina estas jurídicamente, como se ha visto existe mayor regulación de parte de organizaciones civiles y corporaciones.

La segunda, dado que la soberanía se ejerce en una unidad territorial y en principio las redes informáticas y de telecomunicaciones se encuentran fuera de las partes integrantes del territorio, tomando el cuenta los conceptos de legitima defensa y agresión, una forma de presentarse la segunda es la violación de territorio, si hace falta el mismo, en estricto sentido es inexistente un ataque donde un estado carece de soberanía, así es imposible recurrir al principio de defensa legítima.

El problema con estos planteamientos es que mantiene la idea de un mundo material, donde el Estado gobierna invariablemente dentro de sus fronteras, cuando hace mucho que las mismas desaparecieron, aunque de forma figurativa.

Actualmente un gobierno encargado de regir exclusivamente o en parte el ciberespacio es inexistente. La concepción actual del poder del Estado queda corta ante la nueva realidad de la integración mundial, inclusive es imperativo tomar en cuenta factores reales de poder como organizaciones civiles, hackers, corporaciones, que funcionan como medios de control. En este caso, el concepto presenta un problema, ya que el Internet se autodetermina y tiene los medios para definir su estructura así como sus sistemas de control.

El que un Estado particular trate de determinar o regular un área especifica del ciberespacio va más allá de sus facultades soberanas, ya que las consecuencias de su actuar traspasan la aplicación para las redes o individuos ubicados físicamente dentro de su territorio, y afecta a ciudadanos del todo el planeta, como ejemplo, la República Popular China posee filtros de información para el Internet, así la censura a la que somete las comunicaciones y los contenidos el gobierno chino, violenta el conocimiento publico y sobre todo los Derechos Humanos, y afectan inclusive la esfera interna de los individuos; a pesar de ello existen medios técnicos para saltar esas restricciones, aunque su uso constituye delitos en ese Estado.

En el segundo caso, para dar una respuesta, es necesario recurrir a una salida alterna, donde el concepto de territorio se mantenga al margen, es complicado pero de esta forma se puede reconocer que los sistemas y redes estatales principalmente los de gobierno, forman parte de la infraestructura crítica de los Estados y por tanto son una extensión de su personería como ente moral, haciéndolo susceptible de daño, y como consecuencia, cualquier ataque a las mismos será entendida como agresión.

En este orden de ideas, dentro de la guerra cibernética, se toma en cuenta el resultado, las consecuencias y los daños, mismos que invariablemente tendrán nombre y domicilio.

A medida que crece el Internet y las redes mundiales, se hace realidad la eliminación de fronteras, por lo que el territorio adquiere las características de infinito y común; dada esta situación, la cuestión radica sobre la concepción de la soberanía que se tiene desde la paz de Westfalia, en un mundo tan pequeño e integrado será necesario saber quien detenta la misma y donde lo hace.

Algunos autores mencionan que en el ciberespacio se eliminan las delimitaciones globales, geográficas, burocráticas, jurisdiccionales, o conceptuales, situación similar a la fijada para los mercados financieros y monetarios, o inclusive las grandes corporaciones. Algunos piensan que la respuesta es la liberalización del todo en el sistema.

La conclusión es que se hace necesaria la revisión de este concepto y la creación de uno nuevo, que abarque los aspectos más amplios de las relaciones entre Estados en las décadas por venir.

3.3.3 Países Industrializados y en Vías de Desarrollo

A pesar de tener un mundo más integrado, los países cada vez más mantienen una estrecha familiaridad, relaciones más cercanas y hasta intimas, pero las diferencias de clase, de nivel, sobre todo en el campo económico se atenúan cada vez más hasta ser insalvables.

Los Estados poderosos inundan de nuevas tecnologías los mercados, mismas que apenas y se comprenden, las sociedades tardan en adaptarse, pero siguen y forman parte de nuestra existencia; para los países subdesarrollados esto representa una clara desventaja ya que son consumidores netos de tecnología, misma que se entrega bien dosificada, y dirigida específicamente, constituye un medio de control más del sistema de relaciones internacionales.

La enorme oferta y desarrollo de los países poderosos en cuanto a hardware y software, tecnologías de telecomunicaciones, produce una dependencia casi total en relación con los países en desarrollo.

En gran medida, el grado de dependencia tecnológica de los países pobres repercute en una debilidad de sus sistemas, automatizados pero vulnerables, principalmente los militares y de servicios estratégicos.

Poner atención a las características que desde siempre el modelo capitalista ha mantenido para ricos y pobres, es importante, ya que el mismo sistema esta diseñado para que unos pocos ganen y otros pierdan; así los poderosos tienen la capacidad y los recursos para crear nuevas tecnologías, investigar y desarrollar modelos más eficientes para adaptar a sus sociedades a los descubrimientos y de esta forma engrasar la maquinaria del progreso.

En contraste los países en desarrollo consumen tecnología y son improductivos en cuanto a ciencia pura y aplicada en la escala necesaria para ser autosuficientes, esto deriva en un gasto mayor por la compra de la misma, aunado a que las sociedades subdesarrolladas muchas veces desconocen el potencial de lo que adquieren, se adaptan de forma lenta en relación a lo que hacen en el primer mundo, provocando ser presa fácil para que su seguridad, su soberanía inclusive se vea violentada por influencias externas, gracias a las tecnologías que ellos mismos reciben.

Un ejemplo de lo anterior lo podemos encontrar en el software y los ordenadores de importación, que en muchos casos han sido objeto de criticas al encontrar en su funcionamiento programas espías conocidos como puertas traseras que al instalarse permiten la manipulación de la información de la maquina donde se fijan o en el caso del hardware, el ejemplo clásico es el de la impresora manchuria, un dispositivo como cualquiera instalado en una computadora con acceso a Internet, que en su programación contiene un código que al ser completado con un algoritmo, una orden o sentencia informática, explota. Catastrófico y posible.

Pero existen cosas positivas dentro de los países en desarrollo, ya que muchos Estados han echado mano de las nuevas tecnologías para promoverse en el mundo en gran cantidad de aspectos, económicos, políticos, culturales; para aquellos que adoptan las tecnologías como propias y les dan el valor merecido existen gran cantidad de beneficios, siempre y cuando se mantenga una estrecha supervisión de lo que se adquiere.

En el caso de los atacantes poderosos o desarrollados, el uso de la guerra cibernética sirve principalmente como una forma de mantener sus intereses intactos, hace uso de la presión sobre los sistemas vitales de los Estados pobres, los interviene mediante el incremento en la vigilancia y violenta la seguridad interna, corta el suministro de tecnología, actualizaciones de equipos y sistemas de seguridad, aunando a las posibles intervenciones de equipos especiales y utilización de medios de difusión para provocar confusión en la población.

Para los países en desarrollo representa una forma en que pueden limitar las agresiones o intervenciones de los países desarrollados, lograr resistencia y el repudio internacional en contra del agresor, mediante campañas mediáticas y psicológicas principalmente, así como ataques a gran escala mediante el reclutamiento de partidarios y el uso de computadoras zombis, mismas que son operadas de manera remota por pocos operadores expertos, quienes previamente han realizado intervenciones en miles de quipos para manejarlos a su antojo y hacer uso de su poder en un momento determinado.

La división entre los países en desarrollo e industrializados, resulta casi imposible de colmar, por múltiples motivos que pueden ser objeto de trabajos posteriores, la realidad es que la guerra cibernética y sus características permiten que dos puedan jugar el mismo juego.

3.3.4 Ámbitos de aplicación

El ámbito de aplicación de la ley constituye uno de los mayores problemas cuando tratamos de controlar un fenómeno como lo es la guerra cibernética, ya que en principio se carece de leyes uniformes para todos los Estados y a pesar de los intentos de diversos gobiernos para regular de manera local, las implicaciones y relaciones en el ciberespacio necesariamente salen del contorno nacional, afectando inclusive varias regiones.

Tal es el caso de un probable conflicto armado de orden internacional, por dicha situación se hará referencia a los ámbitos de validez nuevamente, al momento que se deja de lado el concepto de ley como norma jurídica por un momento y se piensa en orden jurídico.

Con anterioridad se desarrollo el problema que implica para el Internet como sistema la aplicación temporal y espacial de la ley; toda vez que el ciberespacio, como fenómeno totalizador espacial de relaciones mundiales, y la

guerra cibernética como medio presentan los mismos problemas ya que comparten naturaleza.

Ámbito Temporal.- se recordará que se hizo referencia a la vida de la norma, en este caso, del orden jurídico que se trata de basificar, ya que es insuficiente para el orden internacional elaborar una simple ley para regular cada posible hecho o acto que derivado de un conflicto acontezca en el ciberespacio dado el principio de mutabilidad antes propuesto.

Cualquier intento por establecer una norma concreta o tipificar cada conducta sería insuficiente, por tal razón se pugna por reconocer principios, mismos que atiendan a la generalidad de situaciones que se produzcan y permitan la resolución de controversias.

Ámbito Material.- este se refiere al área del Derecho en que se concentra la ley, norma o para este caso el orden jurídico; crear orden necesariamente requiere de un trabajo conjunto y multilateral con todos los países del mundo, por ende merece atención del Derecho Internacional Público quien será el encargado de establecer normas uniformes para todos los Estados que acceden pretendan el uso de la guerra cibernética en el ciberespacio. Cada país en particular será responsable de realizar la vigilancia y aplicación dentro de su territorio, más las consecuencias de los actos realizados serán de orden internacional, controvertibles solo en este nivel, sometiéndose los conflictos ante autoridades Internacionales reconocidas.

Ámbito Personal.- indica la persona como sujeto individual al que se dirige la ley, sobre el cual recaen sus efectos por situarse en el supuesto de la norma.

El sujeto será en este caso el operador de los medios cibernéticos, el usuario, el proveedor, la dependencia, organismo o Estado, todo aquel con acceso. Es inevitable decir que cualquiera puede convertirse en sujeto, al momento de ingresar al sistema, inclusive una persona que este carente de acceso y nunca lo haya tenido puede estar sujeto al orden del ciberespacio, cuando sufra las consecuencias de su uso, por ejemplo en el caso de los civiles durante la

guerra cibernética, si se ataca el sistema de energía, cualquier persona física puede sufrir daños por la falta de la misma, lo que le daría en teoría el derecho de exigir el resarcimiento del daño. Por tal motivo, los principios son aplicables a todos, ya que todas las redes se encuentran interconectadas.

Ámbito espacial.- posiblemente la que presenta mayores problemas, en el caso de la guerra cibernética, los Estados tienen un gran problema ya que es complicado definir un territorio para el ciberespacio, siendo que el mismo solo es soportado por los sistemas que lo contienen. Ejemplificando un problema, un acuerdo internacional suscrito entre los países de América Latina carecería de poder vinculatorio para cualquier otro Estado, por lo que estos últimos mantienen su acceso pero sin someterse a las reglas establecidas para los suscriptores.

Nuevamente señalamos que se requiere de principios internacionales que desarrollen un orden jurídico internacional aplicable a todos los Estados del planeta ya que sería contradictorio permitir el establecimiento de un orden jurídico local y uno internacional para el ciberespacio, provocaría en mayor medida conflictos de territorialidad, por el principio de libre asociación e intangibilidad del espacio, varias redes interconectadas, de múltiples lugares del mundo, sin orden local específico, en un espacio netamente virtual.

La forma de lograr eficacia será entonces el conocimiento de estos principios y su desarrollo, así como una educación responsable en cuanto al uso del ciberespacio.

3.3.5 Diferenciación de la Guerra Convencional

Existen múltiples razones que convierten a la guerra cibernética en un fenómeno singular y lo separan de las demás clases de conflictos bélicos, la siguiente lista solo menciona algunas diferencias generales, dado que el fenómeno evoluciona de forma alarmante.

- La guerra cibernética implica un nuevo giro en relación con la guerra convencional, ya que anteriormente se encaminaba a producir la mayor cantidad de bajas en el ejército enemigo, diezmar fuerzas y conquistarlo; esta nueva forma implica una respuesta al clamor social de lograr victorias con el mínimo de enfrentamientos, mínimo de bajas y mínimo de recursos.

-La efectividad de la guerra convencional radica en el mayor volumen de recursos, efectivos militares y armas de destrucción más avanzadas que se tenga a disposición. La guerra cibernética es eficaz porque mantiene una mejor capacidad de organización y mando, información y comunicaciones.

--Los elementos clásicos de la guerra se encuentran presentes, únicamente se representan de forma distinta. El espacio territorial es ahora el ciberespacio. Los materiales y conocimientos, es decir las armas, poseen un grado de avance inusitado. El elemento humano debe contar con un nivel de especialización mayor. La capacidad de acción colectiva pierde poder ante un fenómeno que pude mantenerse sin que los ciudadanos se enteren.

-La estrategia en la guerra actual radica en la mejor tecnología en armamento y el uso de millones de datos para tomar mejores decisiones, recursos, mando y control. En la guerra convencional, lo importante es el volumen del ejercito y la capacidad física de los soldados.

-En la guerra convencional, la agresión se comprende como todo aquel uso de la fuerza armada en contra de la integridad territorial, independencia política o soberanía. En la guerra cibernética, nos encontramos con el problema de que carece de territorio material definido, ¿donde termina un Estado y comienza otro?; además, ¿existe soberanía en Internet?, si ningún Estado puede legislar de manera local de forma efectiva ¿hay soberanía? ¿ quien la ejerce?; por ultimo, puede un Estado frenar la libre manifestación de ideas o inclusive la presión de grupos externos en un área que no regula, ¿realmente hay independencia política?.

-El tiempo constituye una enorme diferencia, la guerra convencional requiere de un lapso amplio para su preparación, el establecimiento de estrategias y el uso de mecanismos diplomáticos. La guerra cibernética solo necesita algunas horas, inclusive minutos para recabar información, decidir y actuar.

-La duración es cuestión de días máximo y el inicio de la guerra cibernética es inmediato, se requiere de la sorpresa para que un sistema sea vulnerado de forma efectiva.

-La concepción de combatiente en la guerra convencional se refiere a la persona que de manera efectiva esta legitimada para atacar; en la guerra cibernética la necesidad de formar parte de un ejército es solo aparente, cualquier persona con una terminal de computadora, acceso al ciberespacio y los conocimientos para explotarlos, forma parte de la fuerza en combate.

-En el marco de la guerra cibernética existe la posibilidad de que el margen de daño para los no combatientes sea mayor en relación con la guerra convencional. Esta situación deriva de los blancos, que permitiría convertir los ataques cibernéticos en el medio de dominación de un Estado, si se ataca el sistema eléctrico, o de distribución de agua, los afectados y el daño colateral son tanto las tropas enemigas como los millones de civiles que requieren del servicio, lo mismo pasa con hospitales, sistemas bancarios y financieros.

-El daño colateral en la guerra cibernética se amplia, ya que el número de civiles afectados por un ataque que inutilice sistemas vitales puede arrojar millones de afectados. La guerra convencional presenta la existencia de este mismo daño, pero de forma más aislada dado que sus blancos son objetos físicos, y no sistemas.

-Las armas y la información utilizada en la guerra convencional es de alto costo y uso complejo, permisible solo para algunos de forma legal. La guerra cibernética permite el abaratamiento de costos, la información y comunicación esta disponible para cualquier persona con los conocimientos técnicos necesarios.

-Ambos tipos de guerra generan grandes cantidades de información que debe ser registrada, evaluada y analizada, para la toma de decisiones, La diferencia radica en que la guerra cibernética permite una mayor certeza, rapidez y capacidad de análisis, produciendo de esta forma modelos y soluciones más certeras.

4. PRINCIPIOS PARA LA REGULACIÓN DE LA GUERRA CIBERNÉTICA COMO CONFLICTO BÉLICO

4.1 Justificación en la Participación del Derecho Internacional Público

Es imposible circunscribir el presente trabajo únicamente a la sociología, la polemología o la política. Necesariamente, requiere un estudio por parte del Derecho, el tratamiento y análisis del fenómeno de la guerra cibernética debe responder a un estudio jurídico, dado que es el mejor marco de control al que puede ceñirse, tanto por sus causas como por sus efectos.

Que mejor área del Derecho para realizar esta labor que el Internacional Publico, ya que se trata de un acto surgido entre Estados y que concierne a todos y cada uno de los habitantes del mundo, fenómenos globales, tienen consecuencias de dimensiones mundiales.

Dado el estatus de la Internet, la libertad del flujo de información y el crecimiento de las telecomunicaciones, situaciones que desconocen fronteras, se debe responder a sus problemas mediante respuestas multilaterales, surgidas en el consenso mundial.

La desconfianza por el incumplimiento de compromisos diplomáticos es un sentimiento que genera necesidad de elevar a tratado toda resolución o acuerdo internacional y lograr efectividad en su aplicación. Las mismas son producto de diferencias de desarrollo económico, social, jurídico, el lenguaje, cultura, que provocan lentitud en las negociaciones y generan intereses de grupos determinados para limitar los efectos benéficos de la uniformidad en las normas internacionales, escudando sus intenciones bajo la bandera de la invasión de la soberanía.

Afortunadamente el desarrollo que han logrado para el Derecho Internacional Publico la mayoría de países subdesarrollados gracias a su número en las diversas conferencias internacionales, proporcionan la base jurídica necesaria

para lograr el cumplimiento de acuerdos, auxiliándose de principios como el de igualdad , no intervención, coexistencia pacifica, solidaridad y convivencia.

A pesar de los problemas a que se enfrenta esta materia sobretodo por el clima político, se cree que el mejor modo de adecuar la guerra cibernética a un orden jurídico, es la creación de un acuerdo internacional de características coercitivas, derivado de la escasez de respeto que se tiene por las resoluciones de la Organización de Naciones Unidas, las sentencias de la Corte Internacional de Justicia, la jurisprudencia internacional, e inclusive la costumbre, principalmente y como ya se cito, por parte de los países industrializados que son en mayor medida los encargados artífices de este nuevo Estado de cosas en que la información y la comunicación cubren el globo.

Los peligros que derivan de un mundo interconectado hasta el punto más intimo de nuestras relaciones comunes, ya que un mejor entendimiento de la misma permitirá lograr ordenes jurídicos mucho más efectivos que atemperen los posibles daños de su utilización.

De la misma forma, es aceptable una convención, derivado de la gran cantidad de reglas técnicas, convencionalismos y costumbres encaminados a la regulación de los fenómenos informáticos y cibernéticos, el maestro García Máynez al respecto señala:

"La tendencia, siempre creciente, hacia la codificación del derecho, es una exigencia de la seguridad jurídica. A pesar de su espontaneidad, el derecho consuetudinario carece de una formulación precisa, lo que hace difícil su aplicación y estudio. El legislado en cambio, además de su precisión y carácter sistemático, puede modificarse con mayor rapidez, y se adapta mejor a las necesidades de la vida moderna".[58]

Es necesario apuntar que se debe evitar la pugna por la descripción y codificación de cada caso en concreto que la guerra cibernética puede ofrecer,

[58] GARCÍA MAYNEZ, Eduardo, "Introducción al Estudio del Derecho", O*p. Cit.*, Pág. 53

pero los principios que determinen el ser de este hecho, si deben contenerse en un protocolo formal.

Aunque lamentablemente esta propuesta, enfrenta como principal problema la incomprensión profunda de su funcionamiento y posibilidades.

4.2 Bases Aplicables

Después del análisis realizado respecto de la guerra cibernética, así como de los problemas expuestos en relación a su naturaleza y aspectos jurídicos, estamos en posibilidades de lograr bases legales más firmes que se deben atender al momento de la adecuación de un orden jurídico en este nuevo campo.

Para comenzar a resolver este problema se tiene que pensar de la misma forma que lo hicieron los creadores del sistema, la respuesta a la aplicación de la ley estriba en evitar la aplicación dentro del ciberespacio como se conoce la ley en el mundo real, sino hacerlo en dos estadios, uno fuera, sobre la persona y los medios de comisión, y otra dentro del espacio virtual, mediante acciones técnicas que impidan la realización de transgresiones. Para ello es necesario trabajar principalmente con acuerdos internaciones que fijen principios, basados en la costumbre de las propias actividades del ciberespacio, así como en los códigos de ética y de funcionamiento del mismo.

De igual forma se debe tomar en cuenta en todo momento que el reconocimiento del acceso al ciberespacio, es tanto como aceptar el derecho a la información, la libre expresión, la educación, la libre asociación, la protección de datos personales, inclusive garantizar la comunicación entre personas, cuestión puramente natural y necesaria para la vida en sociedad.

En el momento que se garanticen estos derechos fundamentales se estará en posibilidad de forjar un orden más justo. Aquí se exponen algunas propuestas para basificar el desarrollo de este orden jurídico que necesariamente tendrá como consecuencia la elaboración de un acuerdo internacional.

-Orden jurídico. Un orden jurídico esta compuesto de mucho más que normas, implica una estructura de control que guía la conducta externa de los individuos, sin el cual no puede existir una sociedad. Cualquier sistema tiene como principio de funcionamiento el orden, cuando el mismo es inexistente, el sistema falla, ya que no responde a la necesidad para la cual fue creado, el que se genere un orden especifico para el sistema no es para limitar su funcionamiento, sino para evitar y corregir estos errores.

Es erróneo pensar que un orden para el ciberespacio constituye una limitación a los derechos y libertades que representa; ya existe un orden y normas aun sin escribir o codificar, que adecuan las relaciones en el ciberespacio, únicamente hace falta la forma jurídica y su reconocimiento, es decir legitimación.

El orden que se busca para la guerra cibernética y por ende el ciberespacio debe descartar la restricción de libertades, y permitir la ampliación de acceso y flujo de información, de manera que todo el mundo pueda aprovechar sus beneficios, bajo el marco estricto de respeto a los derechos humanos, al tiempo que garantice la seguridad de todo el sistema.

-Reconocimiento Internacional. Con la finalidad de lograr normas de derecho internacional uniforme, hay que reconocer el peligro que representa la guerra cibernética, sin pensar por el momento en el número de bajas o la sangre que se derrame, existe mayor posibilidad de que cause daños materiales irreparables, tanto al estado agredido, como a todos los usuarios del ciberespacio. Si un solo país o sujeto internacional lo toma en cuenta es insuficiente, pero siempre un buen comienzo para reflexionar en las implicaciones mundiales del fenómeno.

-¿Res communis o res nullius? El ciberespacio al igual que las aguas internacionales, debe ser tratado como la cosa de todos, donde cada Estado, organismo, ente o simplemente usuario, pueda acceder sin restricciones y con la seguridad que brinde el propio sistema, sin temor a sufrir daños, bajo la

obligación de mantener vigilancia constante en su propia esfera de acción ante acciones antijurídicas en red, así como el manejó responsable de sus recursos. Sería un retraso sectorizar o considerar este espacio virtual como res nullíus o inclusive propiedad privada, ya que cada acción que se genera en un ordenador, red o sistema, afecta invariablemente al todo.

-*Supresión de la Brecha tecnológica o digital***,** es importante dada la necesidad de descartar las diferencias existentes entre los distintitos Estados a fin de garantizar un acceso a la información y la comunicación, que permita el desarrollo global. Si se espera lograr el principio de igualdad, solidaridad y desarrollo para la comunidad internacional, las diferencias científicas y tecnológicas deben ser suprimidas con el fin de lograr bienestar.

- *Eliminar la Movilización Electrónica Transnacional* como recurso de agresión. Un asunto doméstico en cualquier país puede convertirse en un asunto de relevancia internacional gracias a la difusión que permite el ciberespacio. Con mayor razón en este tiempo de integración mundial es comprensible que se presente este fenómeno que deriva en la participación de fuerzas y grupos sociales y de Estados a favor o en contra de determinada causa, es por ello que se recurre a este tipo de difusión al más puro estilo de la propaganda de guerra, a fin de encontrar adeptos en la comunidad internacional y la sociedad global. La limitación envuelve únicamente los efectos nocivos de la agresión, ya que cuando es utilizada la movilización con fines humanitarios presenta un auxilio con posibilidades de crecimiento exponencial.

-*Tratados Internacionales jurídicamente vinculantes.* La guerra como generalidad y la guerra cibernética, como tipo o rama de la misma, hechos eminentemente sociales, humanos, van más allá de las regulaciones y codificaciones jurídicas, a pesar de existir una prohibición expresa para su uso, su reconocimiento esta implícito, desde la misma doctrina de guerra y la división natural del Ius in Bello y el Ius ad Bellum, se entiende prácticamente imposible de eliminar, solo limitar sus efectos hasta en tanto el concepto de soberanía se separe de los Estados particulares y se desarrolle la soberanía de la comunidad internacional y la guerra solo sea un recuerdo.

Por esta situación, aún es necesario que cada apreciación, cada principio o norma que se establezca en el sistema internacional con referencia a este fenómeno, debe constar en un tratado internacional cuya fuerza obligatoria garantizara su cumplimiento.

-*Cooperación internacional,* es un principio invariable ya que este es el primer paso para reconocer a un atacante, el lugar de donde proviene, sus motivos, fines, recursos y posibles aliados. Recordemos que el ciberespacio es un conjunto de redes, y las mismas tienen base en estados muy diversos, los ataques evitan la lógica lineal, por el contrario, las máquinas siempre buscan la mejor ruta, ser más rápidos, efectivos y dejar el menor número de rastros. Una comunidad de Estados y organismos de seguridad en Internet, tienen más facilidad para resolver estas interrogantes en conjunto, al contrario de si operan solos.

El que un solo Estado regule la totalidad del ciberespacio, limitándose exclusivamente a su territorio, deriva necesariamente en la creación de un filtro constante, cuyo afán de producir seguridad se presta para violaciones a derechos dentro de la población del mismo e infaliblemente mantiene un margen de aberturas inevitables, ningún sistema es seguro al cien por ciento. Dada esta situación la cooperación, el esfuerzo conjunto debe darse.

-*Agresión.* Este concepto en sentido general es la base de toda guerra, inclusive la cibernética, es un presupuesto para que exista el conflicto bélico, *c*on anterioridad se cito su definición, recordemos que se trata de el uso de fuerza armada contra la soberanía, integridad territorial o independencia política. Ahora la importancia radica en conocer si es aplicable este termino a la guerra cibernética o es necesario forjar algún otro.

El uso de la fuerza se reconoce como el ejercicio de coerción ya sea militar, económica, política o de cualquier otra índole, que atente contra la soberanía, la independencia política o territorio de un Estado.

Este uso de la fuerza será armada cuando utilice como medios instrumentos que inflingan daño a las personas o las cosas.

La soberanía, la integridad territorial e independencia política son conceptos reductibles a cualquier aspecto que suponga una intervención indeseada, como forma de presión.

En este orden de ideas, el concepto de agresión reconocido por los países miembros de la Organización de Naciones Unidas, contiene de forma adecuada, dada su amplitud, a la guerra cibernética, es innecesario el acuñar uno nuevo. Este fenómeno cumple con el requisito de uso de la fuerza, su utilización provoca coerción sobre un Estado, además, a pesar de no contar con instrumentos físicos, los programas informáticos que utiliza son verdaderas armas, mismas que causan de manera directa un daño a lo sistemas cibernéticos y por ende uno colateral a las personas.

El segundo elemento se colma a la perfección ya que toda incursión en los sistemas cibernéticos sin el consentimiento de el estado agredido implica un atentado a la soberanía, la independencia política o el territorio.

Ante estos tres puntos, también hay que tomar en cuenta, que si bien es imposible hablar de violación física al espacio donde afectivamente se autodetermina el orden jurídico de un estado, o se desarrolla un sistema político, es decir el territorio considerado nacional, y tampoco existen tropas regulares, entendiendo por estas inclusive un solo soldado uniformado y pertrechado en territorio extranjero, si existe invasión, interrupción o ingreso sin autorización a sistemas y redes locales sin consentimiento del Estado que los mantiene, por tanto la violación se colma, ya que deriva del uso de fuerza irresistible en contra de otro.

En cuanto a la relación de la agresión en el supuesto de la guerra cibernética y la defensa legítima, la Carta de Naciones Unidas aplica a la perfección en el caso ya que el Estado agredido puede responder una amenaza de manera subsidiaria y provisional; así mismo cumple con el requisitos teóricos de

necesidad e inmediatez , la única posible variación será en el caso del deber de informar, ya que este principio depende de una velocidad casi instantánea, de lo contrario, las huellas del ataque pueden ser degradadas rápidamente en el transcurso del tiempo.

Uno de los puntos importantes es establecer que una intromisión de un solo hacker o cracker, inclusive de un Estado naturalmente enemigo o algún puñado de ellos, no puede considerarse agresión como base de conflicto bélico, por el contrario, su avanzadas, funcionan como alertas anticipadas para los Estados que los padecen, ya que el permitir estas incursiones muchas veces proporciona ayuda para identificar los puntos débiles de los sistemas.

Entonces deberá entenderse la agresión en el marco de la guerra cibernética cuando exista un ordenador o redes de los mismos, que utilicen medios complejos de intervención y ataquen un sistema local poniendo en peligro la operabilidad, funcionamiento y sostenimiento del mismo

-*Competencia y jurisdicción.* La competencia se comprende como:

"…el ámbito, la esfera o el campo dentro del cual un órgano de autoridad puede desempeñar validamente sus atribuciones y funciones"[59]

Es decir es el ambiente donde un órgano, legislativo, judicial, administrativo, ejerce efectivamente sus funciones. Es necesario recordar su división en cuatro tipos, grado, cuantía, materia y territorio; esta última representa el espacio geográfico, determinado territorio físico donde un órgano ejerce validamente sus funciones, y es la que más interesa para este estudio.

En el mundo actual es difícil distinguir los límites de competencia territorial en los cuales encuadra la realidad de la guerra cibernética en un orden jurídico, ya que en el caso del ciberespacio estos límites son más flexibles, inclusive invisibles, por tanto es complejo dirimir que reglas aplican y en que lugar.

La jurisdicción por otro lado es:

[59] GÓMEZ LARA, Cipriano, "Teoría General del Proceso", *Op. Cit.* , Pág. 145

"…función soberana del estado, realizada a través de una serie de actos que están proyectados o encaminados a la solución de un litigio o controversia, mediante la aplicación de una ley general al caso concreto controvertido para solucionarlo o dirimirlo."[60]

Como se aprecia este concepto se refiere a la capacidad de un Estado para establecer un determinado orden jurídico y aplicarlo para cada caso concreto que requiera resolver una controversia.

Para el caso de la guerra cibernética, es importante conocer estos conceptos generales ya que se requiere saber que Estado o Estados tienen la facultad para establecer un orden dentro del ciberespacio, y a quienes obligará ese orden, además de conocer en que territorio se aplicarán.
En cuanto a la competencia, se reitera que hasta hoy ningún Estado organismo o sujeto de derecho internacional ha determinado hasta donde llega o que comprende el ciberespacio, o en su defecto, ni ha sectorizado un área determinada donde este ejerciera un poder único, por tanto es importante proponer quien y donde se aplicará el orden jurídico por establecer.

El ciberespacio es un área, susceptible de relaciones y conductas humanas por tanto sujeto al derecho. Además esta zona tiene dos ámbitos, el interno que se comprende como el sistema virtual; y el externo, el territorio, el espacio geográfico donde las consecuencias de su uso se materializan, afectan de forma directa o colateral. En el interno, los sistemas lo componen las redes y sistemas cibernéticos, conectados entre si, el externo se refiere a las cosas o personas en los cuales produzca consecuencias.

En cuanto a la jurisdicción, es imperativo saber quien se encargará de la aplicación del orden; para lo cual creemos importante la creación de un área especializada dentro de la Organización de las Naciones Unidas y de la Corte Internacional de Justicia, integrados por delegados de cada país, así como expertos de la sociedad civil, comunidades virtuales, organismos no gubernamentales, técnicos y científicos, quienes tendrán la función de vigilar el desarrollo de la guerra cibernética, así como de lograr criterios uniformes para la regulación de su uso y reducción de sus efectos

[60] *Ibidem*. pág. 97

Este órgano deben tener autonomía y mando, así como facultad para ejercer y legitimar el uso de la fuerza cibernética. Es obvio decir que dada la naturaleza sorpresiva e inmediata de la guerra cibernética es imposible tomar en cuenta todos los aspectos de una agresión y dar una opinión o voto para autorizar represalias en unos cuantos minutos, por lo que el Estado agredido deberá mantener su derecho a la autodefensa.

En el caso de la legitimación del uso de la fuerza, el repudio a las hostilidades, inclusive la toma de medidas en contra del agresor, como pueden ser la limitación de su accesos al ciberespacio, se requiere un pronto consenso que la misma inmediatez del Internet permite, es decir que el aprovechar el ciberespacio en máxima capacidad permitirá la toma breve de decisiones.

Una vez terminado el conflicto, queda en mano de la Corte Internacional la solución de controversias y la aplicación de sanciones a los responsables.

-Ámbitos de validez. En primer termino el orden jurídico debe ser atemporal, adaptable, principios generales aplicables en todo momento y mutables de acuerdo al avance tecnológico.

Por lo que hace al espacio, el orden debe ser global, internacional, en cuanto a la comisión de las conductas; con vigilancia local en el territorio tangible de cada Estado para los efectos. Así una conducta antijurídica que se desarrolle en el ciberespacio es susceptible de detectarse mediante sistemas de vigilancia alrededor del globo, pero la reacción necesariamente será local, tanto del lugar de donde se produjo dicha actividad, como de los lugares donde se presentaron las consecuencias.

Por lo que toca al ámbito personal, el orden sujetará a todos los usuarios, gobierno, organismos oficiales y extraoficiales, dependencias, empresas, proveedores de servicios; cualquier persona, física o moral con acceso al sistema, que haga uso de los recursos del mismo u obtenga algún aprovechamiento, o que a pesar de carecer de acceso reciban un daño producido por su uso, siempre que este resulte en consecuencias de tipo internacional. Por ejemplo, el fraude electrónico o el robo de dinero de un banco realizado en México con consecuencias para mexicanos con domicilio

en el territorio nacional necesariamente se refiere a un delito local. Pero en el caso de la guerra cibernética, los daños producidos a los ciudadanos de un país van más allá de la cuestión local y trascienden al plano internacional

En el ámbito material, necesariamente compete al Derecho Internacional Publico y la comunidad internacional.

-*Combatientes.* En la guerra convencional es posible determinar quien combate y quien no, pero la guerra cibernética da un giro, ahora los combatientes deben ser reconocidos como aquellos que estén a cargo de los ordenadores, redes o sistemas implicados en agresiones internacionales, incluyendo a aquellos grupos de mercenarios informáticos. Para el caso de computadoras controladas a distancia, deberá existir responsabilidad en contra los proveedores de servicios que con conocimiento de causa permitan estas actividades.

-*Intrusión en sistemas y robo de información.* Es difícil catalogarlo como agresión ya que el daño comprobable e inclusive rastro de el si se realiza de forma furtiva, pero si hay una violación a sistemas de seguridad. En estos casos el daño no es la medida de la agresión sino la intervención violatoria de sistemas, la exposición al peligro y estabilidad de estos.

-*Justificación para garantizar la seguridad, la vigilancia y la intimidad en el ciberespacio***.** Aún es difícil saber que base deben mantener estos actos para dejar intacta la esfera personal de las personas sin renunciar a la seguridad nacional. A parte de los conocidos sistemas de identificación y criptografía, de los que se mencionará algo más adelante, se debe seguir con las siguientes pautas; educación y responsabilidad en el uso del ciberespacio; vigilancia sectorizada y coordinada; cooperación internacional para el intercambio inmediato de información; sistemas de detección inteligente de amenazas y graduación de las mismas.

-*Secretos Industriales, bases de datos gubernamentales y sector privado.* Las consideraciones para la guerra cibernética abarcan la personería de los Estados en tanto sujetos del derecho internacional, pero el crecimiento tan

tremendo de las corporaciones es imperativo tenerlo en cuenta, por ello la cooperación internacional debe tender a regular de forma estricta el aprovechamiento del ciberespacio para fines comunicativos, de información, culturales, científicos, intercambio, y regular tanto en el ámbito internacional como el local el comercio en línea.

Las actividades ilícitas como el robo de secretos industriales y bases de datos gubernamentales en ultima instancia deben ser responsabilidad de los depositarios de dicha información. En el caso de los datos personales que obran en archivo de gobierno, existe una obligación directa de parte del órgano gubernamental que por descuido, negligencia, impericia u otra falta de atención, permita o facilite estas actividades.

-*El papel de los Proveedores de Servicios de Internet* es importante ya que para la mayoría de ciberciudadanos, el acceso al ciberespacio es mediante estas compañías, para hacer uso de cualquier servicio o red, es necesario coordinar el ordenador y sus recursos en la dirección deseada. Por esta situación la regulación adecuada y vigilancia de parte de los Estados en tanto que resultan en su mayoría ser entes privados; así como los diversos grupos que mantienen el sistema en operación, es una necesidad, tanto en las cuestiones de concesión de operaciones como en la cooperación jurisdiccional. Sobretodo si tenemos en cuenta que el espectro radioeléctrico, las ondas y frecuencias que lo componen, los medios y vías de las comunicaciones y la información, se consideran en la mayoría de los países como parte del Estado y propiedad de las naciones, regularmente concesionados a los entes citados.

4.3 Seguridad y Gobierno en Internet.

Las nuevas tecnologías y en particular el uso del Internet, han otorgado una libertad inusitada a los usuarios del ciberespacio, derivado principalmente de la posibilidades tan serias que otorga una navegación anónima, el intercambio libre de contenidos, la recopilación de información de interés, la libre manifestación de ideas y sentimientos.

Lamentablemente, y como se ha desarrollado en este trabajo, existen claras situaciones que dan la muestra para pensar en el manejo negativo de dichos medios, en este caso, la proliferación de ataques a sistemas cibernéticos de otros Estados, sin dejar de lado otros problemas de relevancia, como los delitos informáticos, fraudes electrónicos, la proliferación de pornografía ilícita, ciberterrorismo.

A fin de determinar pautas que permitan el libre desarrollo y ampliación de estos sistemas para beneficio de todos los habitantes del planeta y se evite en mayor medida el uso indebido de las redes, es necesario apuntalar algunas ideas.

Existen tres conceptos muy importantes, que escapan de la formalidad , insuficientes para la realidad actual por lo que responden a una conceptualización propia son la seguridad, la vigilancia y la intimidad:

Se entiende a la *seguridad* como la confianza o sensación absoluta de certeza que se sostiene con respecto a una cosa, persona o situación.

La seguridad en el ciberespacio estriba en la certeza que tienen los usuarios de que su navegación y relaciones escaparán de afectaciones generadas por agentes externos; depende en gran medida del uso de contraseñas, códigos o palabras clave necesarias para acceder a un sistema o sitio determinado; y muros de fuego, que son programas que protegen un ordenador o sistema de la entrada prohibida de usuarios no autorizados; ambos están encaminados a lograr cierto nivel de confianza para que el ciberciudadano que forma parte de la infoesfera resulte invulnerable para actividades indebidas, restringiendo el acceso a datos y áreas criticas del sistema.

En la guerra cibernética, la seguridad va más allá del principio de seguridad nacional, que evoca la idea de certeza en la continuidad o vida de un Estado determinado y su forma de vida. Una de las más importantes áreas de desarrollo de los Estados son las tecnologías de la información y comunicaciones, para mantenerlos es necesario contar con mecanismos que impidan perder la certeza de que dichos sistemas estarán siempre disponibles.

Es por ello que cada Estado utiliza del modo más conveniente estas tecnologías y trata de fortalecer sus sistemas internos, de esta forma garantiza un mínimo de funcionalidad en caso de una intervención militar. Dado que el ciberespacio es un área imposible de clausurar sin tener como consecuencia la limitación de información y comunicaciones, se intenta blindar sectores específicos.

La *vigilancia* es la conducta dirigida a la extrema atención en los detalles actitudes y comportamientos de un sistema, con el fin de influenciarlo o controlarlo.

En el caso de esta conducta llevada a cabo dentro del ciberespacio nos interesa saber que la misma esta organizada en mayor medida por organismos civiles, de expertos, autónomos, así como gobiernos, que en su mayoría desean mantener el control del ciberespacio y encuentra en esta una forma de manejar a la población o a grupos de la misma, y logran así dirigir sus conductas de una forma determinada.

La vigilancia moderna ha roto las barreras de la intimidad como nunca antes en la historia, y es tan amplia debido a los medios tecnológicos actuales, computadoras, teléfonos celulares, dispositivos móviles diversos, geo posicionamiento global, satélites, nanotecnología, documentos que integran datos biológicos y conductas diversas como el análisis conductual, y el espionaje, por lo cual es virtualmente imposible escapar de ella.

La vigilancia en la guerra cibernética posee una importancia toral, ya que los sistemas son más vulnerables a las sorpresas, por lo que una atención adecuada puede permitir un ataque, limitarlo e inclusive revertirlo; debe recordarse que la velocidad a la que ocurren estas intervenciones muchas veces es suficiente para realizar un reclamo dentro de las reglas actuales del sistema internacional, por ejemplo, recurrir a la legítima defensa implicaría dar aviso al Consejo de Seguridad de la Organización de Naciones Unidas, pero en dicho proceso el ataque tal vez se haya consumado; se auxilia principalmente de métodos dirigidos a la captura de información fidedigna que ponga en

problemas la seguridad del enemigo y permita mejorar las decisiones y el mando propios.

Intimidad es el ámbito particular de un ser humano en el que se desenvuelve de manera personalísima el desarrollo esencial de una persona a la cual no tiene acceso alguna otra sin permiso de la primera, de igual forma es un derecho fundamental oponible a agentes externos. Es un espacio intrínseco de cada sistema en general, que contiene los datos, las características más precisos y únicas de lo que es o representa, su particularidad, su individualidad.

Para el ciberespacio, la intimidad representa la posibilidad de que un usuario o ciberciudadano evite ser reconocido si es su deseo, soslaye la posibilidad de que cualquier otro invada esa área interna, y haga mal uso de la información que contiene, e inclusive juzgue su conducta y realice actos de agresión en su contra.

En la guerra cibernética, la intimidad se refiere al cuidado de los sistemas críticos internos, que deben mantenerse en línea, pero lejos del peligro de una agresión, y servir únicamente para propósitos del Estado que los posee.

Muchas veces la extrema vigilancia produce violaciones a la intimidad de las personas, teniendo como consecuencia el nerviosismo de los demás sujetos y por ende la perdida de confianza, perdida de seguridad.

Un claro aumento de la vigilancia necesariamente repercute en la intimidad, ahora existen muy variadas regulaciones o normas que obligan a los individuos de un Estado a sujetarse a registros de donde se obtienen datos personales y demás información de tipo personalísima. De acuerdo a los gobiernos la misma esta resguardada y posee sistemas de resguardo, pero eso aún permite la corrupción que hace uso de estas bases de datos para venderlas al mejor postor.

Las tecnologías cibernéticas permiten que se remitan por el ciberespacio vía líneas de comunicación u ondas en el aire mediante ondas de diversos frecuencias, estos tipos de información personal; las llamadas a celulares,

envíos por Internet de documentos, números de tarjeta de créditos, cuentas bancarias, son claros ejemplos de datos libres en los sistemas, a la mano de la persona que tenga el equipo y el conocimiento para explotarlas, se viola de este modo la intimidad de las personas, se evita la vigilancia y destruye la seguridad.

La información que en su mayoría se sustrae del ciberespacio es irreductible, ya que para la guerra cibernética cualquier inicio o debilidad en un sistema es importante, secretos militares e industriales, ubicación de bases y sistemas críticos como electricidad, agua, sistema financiero y bancario, tele comunicaciones; funcionamiento de los mismos sistemas, inclusive datos logísticos, poblacionales y personales.

Para lograr la ansiada seguridad en el ciberespacio, deben entenderse los métodos mediante los cuales se lograra fortalecer el creciente flujo de información y convertirlo en contenidos inviolables, dichos medios son principalmente la identificación de los usuarios y la criptografía.

La identificación obedece en el mundo real a los rasgos que se utilizan para determinar o localizar a un individuo evitando la suplantación. En el ciberespacio se eluden los rasgos físicos, pero la identificación de usuarios se realiza mediante firmas digitales, que son códigos complejos cuyo uso solo pueden incumben al emisor y al receptor.

El método más efectivo de lograr seguridad en los sistemas es mediante el sistema de identificación, que fija firmas digitales para cada usuario, cada persona que acceda al sistema posee una clave, en todo momento y desde cualquier lugar del mundo se puede saber si alguien ingresa a las redes y cada paso que realiza, más dicho sistema escapa de la legalidad porque hacer esto permitiría la violación de derechos como la multicitada intimidad, a la vez que elimina la diversidad de la información y limita la libertad de expresión así como el libre intercambio.

La propuesta esta encaminada a que la identificación sea exclusiva de los proveedores de servicios que operan en estos sistemas, mismos que deben obedecer a los más altos estándares de conducta ética, ya que en sus manos

tienen la intimidad de las personas. Estos proveedores mantendrían registros privados de usuarios similares a los utilizados en el sistema financiero, a los que se puede acceder únicamente mediante orden de órgano competente.

Los datos que se registren deben obedecer a principios de transparencia bien definidos, además de permitir correcciones y aclaraciones, con las debidas providencias, sanciones y el reconocimiento de acción en contra de el mal uso de los mismos; en caso de uso indebido de dichos datos deben crearse las pretensiones resarcitorias adecuadas que impliquen inclusive réplicas y reestablecimiento de la fama pública.

Para el caso de una guerra cibernética se puede pensar que esta medida es insuficiente, ya que la guerra es un fenómeno impredecible y se separa de la legalidad, más es de suma importancia para lograr la identificación plena del o los agresores, y por ende el uso de represalias, evitando el daño a Estados ajenos.

Lo más importante es permitir el análisis del comportamiento de estos proveedores de servicios por parte de organismos internacionales y organizaciones civiles de notoria calidad moral, para dejar de lado el nivel de corrupción que impera en muchos Estados, ellos serían a fin y al cabo quienes den el visto bueno para la operación de servicios en el ciberespacio.

La *criptografía* se refiere a la codificación y encriptación de información, haciéndola inaccesible para todo aquel que carezca de la clave. Permite altos niveles de intimidad y anonimato en los sistemas cibernéticos.

Para la guerra cibernética, mantener altos niveles de seguridad en los flujos de comunicación, privacidad en las comunicaciones y vigilancia de los individuos, tanto nacionales como extranjeros, dentro de las redes y sistemas informáticos es crítico.

Los Estados y pocos organismos internaciones tienen la llave de la información que circula por el ciberespacio, por lo que la labor tanto en tiempo de guerra como de paz repercute necesariamente en un trabajo de equilibrio y coordinación, mantener estándares altos de moralidad para evitar invadir la

intimad y libertad de los usuarios, de los ciberciudadanos, al mismo tiempo que vigila las entradas y salidas de información estratégica, el comportamiento de los sistemas, la regulación de los administradores de redes y los proveedores de servicios con el único propósito de prevenir y repeler en caso de que sea necesario una agresión por esta vía.

Dentro de los sectores más radicales del ciberespacio se reconoce a la vigilancia como un acto violatorio en si mismo, y se tiende a limitar su uso, más es factible señalar que mientras la vigilancia sea realizada apegada a derecho, con la mayor discreción y atendiendo a lo que se busca exclusivamente sin detenerse en otras posibles conductas, puede desarrollarse en un plano de legalidad, pero debe reconocerse el derecho de los usuarios a la utilización de tecnologías de encriptación y codificación avanzadas.

El problema se presenta ante al principio que muchos Estados argumentan, la seguridad nacional, motivo suficiente para violar derechos humanos, inclusive requieren mantener a todos lo usuarios aislados y monitoreados.

La creencia de supeditar los intereses del Estado frente a la vida y libertades de los individuos es cuestión antigua y compleja, ya que en estricto sentido, la supervivencia de estado mantiene una jerarquía superior, inclusive constituciones como la mexicana prevé suspensiones de garantías frente a casos como las intervenciones armadas.

Más allá de tratar de limitar la vigilancia estricta de los sistemas *solo en tiempos de guerra,* o de pugnar por la liberalización de todo sistema cibernético, y evitar mecanismos de control, es imperativo una adecuación de la conducta humana basada en la educación, la cultura y por supuesto la adaptación a las tecnologías cibernéticas; sobre todo permear a los ciberciudadanos y ciudadanos del mundo de la cultura de buena vecindad, cooperación y respeto a la diversidad, no intervención y legalidad.

Esto tendría como resultado el mejoramiento y comprensión de los sistemas de seguridad; evitaría el aumento de activistas anárquicos, expertos sin nacionalidad definida con capacidad de ataque; el ingreso de intrusos a bases

de datos privadas e información critica; robo de claves criptográficas, contraseñas y en general la violación de sistemas.

Por lo que hace al gobierno del ciberespacio, es verdad que el mismo compete a Estados, organizaciones civiles, particulares, corporaciones y organismos internacionales autónomos, que se encuentran en un plano de poder similar al de las grandes transnacionales y pugnan por el reconocimiento como sujetos del Derecho Internacional.

En el ciberespacio se impide reconocer el termino gobierno para este esfuerzo de mantenimiento, desarrollo eficaz y uso adecuado del sistema, ya que entiende como gobierno electrónico al que se realiza en línea, que sostienen los poderes formales del Estado, encaminado a la aplicación de políticas dirigidas a la administración y regulación de los servicios y el mejoramiento de la relación gobierno gobernado. Es por ello que en el argot cibernético se ha acuñado el concepto de gobernanza.

La *gobernanza* es el acto multilateral de administración del ciberespacio como hecho, entiende la importancia de una toma de decisiones internacional, con todos los usuarios y representantes necesarios, que garantice el adecuado funcionamiento del las redes que conforman el sistema, así como su crecimiento, desarrollo, y acceso libre universal. Inexistentes son los poderes formales ya que se reconoce la igualdad de todos los actores, que trabajan en metas comunes y reconocen la independencia del ciberespacio como hecho ajeno a voluntad única.

En algunos círculos incluso se pretende la vuelta a la democracia griega, donde todos tenían voz en el ágora, ya que hoy en día es posible la idea, pero si limitada por la seguridad del sistema.

La *democracia electrónica* es un concepto que se relaciona con los esfuerzos encaminados a permitir y ampliar la participación ciudadana en las redes mediante su libre acceso y la relación con sus representantes.

La realidad es que si pensamos en gobernanza en Internet es complicada su implementación; lo que más se acerca a una regulación, administración del mismo es por ejemplo la asignación de nombres de dominio, el establecimiento de los estándares de la arquitectura del Internet que funciona en redes interconectadas, o el uso generalizado de protocolo TCP/IP.

Otra cuestión importante es que actualmente el control del sistema obedece a organismos y personas físicas, reconocidas en el ámbito informático y de comunicaciones, hasta ahora su control ha sido mantenido, sin la mano de los gobiernos del mundo, hecho que a simple vista es bueno ya que impide el intervencionismo estatal pero dejar en manos de particulares algo con tanto potencial , inclusive bélico, es un poco descuidado, por ello un gobierno mundial y los ciudadanos del mundo deben regir el Internet y demás sistemas, dando pie a una participación integral.

Se reconoce en todo momento el papel de los organismo internacionales reguladores que permiten el funcionamiento libre del Internet como se conoce y en caso de falla masiva o inclusive mal uso generalizado de lo sistemas, reaccionan con cortes o limitaciones a la conectividad, lo que tiene bondades y desventajas, ya que se limita la agresión pero se interrumpe la integración al mundo actual.

Un ejemplo de esto se encuentra en la Carta de la Asociación para el Progreso de las Comunicaciones sobre Derechos en Internet, que reconoce la gobernanza, y otros principios para el ciberespacio:

- Un gobierno multilateral y democrático sin preeminencia de estado alguno , abierto y accesible para todos.

-Internet descentralizado, ínter operable y colaborativo.

-Arquitectura y estándares abiertos. Cualquier red se puede conectar siempre y cuando obedezca el protocolo estándar TCP/IP.

-Soslayar filtros de contenido, invasión de privacidad y creación de intranet nacionales. Se debe evitar la fragmentación de Internet y la limitación de libertades en aras de una supuesta seguridad total. [61]

Para la guerra cibernética es importante crear tal y como establece el documento en comento un gobierno multilateral que homologue sistemas, para que durante un ataque, existan rastros fidedignos comprobables por varios de sus integrantes y de manera inmediata se tomen medidas para limitar la agresión sin desconectar al agredido; que se permita la identificación rápida y oportuna así como el derecho a la defensa legítima.

Permitir el crecimiento del ciberespacio al tiempo que se impide que Estados diversos pretendan estar conectados y a su vez mantener redes internas o nacionales controladas en su totalidad, de esta forma se mantiene un nivel adecuado de habitabilidad en línea, disminuyendo la posibilidad de una intervención.

4.4 Participación de los Estados; Sector Privado y Sociedad Civil

Como se ha establecido, la participación de los sectores estatal, privado y social constituyen los pilares sobre los cuales descansa la obligación de desarrollar pautas generales aplicables al fenómeno de la guerra cibernética, los ciberciudadanos y la sociedad mundial apuestan a la creación de una comunidad basada en los mismos principios y fines, que evite la sectorización de la información y de las comunicaciones, así como la eliminación de las armas cibernéticas y las hostilidades dentro de los sistemas, buscan la libertad en su máxima expresión dentro del ciberespacio, con la dosis justa de responsabilidad en su aprovechamiento.

Dada esta situación se analizan diversas cuestiones con respecto al rol que debe desempeñar cada actor dentro de esta nueva realidad.

[61] ASOCIACIÓN PARA EL PROGRESO DE LAS COMUNICACIONES, "Carta sobre Derechos en Internet" , Abril 2009
http://www.apc.org

La problemática de la participación de los Estados en la guerra cibernética deriva de su calidad, en estricto sentido, solo ellos tienen la capacidad llevar a cabo empresas de tal envergadura y buscar la dominación de otro Estado mediante su uso.

Tomando en cuenta el abismo tecnológico en que el mundo se encuentra dividido, el primer paso es la eliminación de la brecha digital o tecnológica, ya que es imposible hablar de una igualdad de criterios entre Estados desiguales; con esto se pretende elevar el nivel de desarrollo técnico científico de todos los países, o en su defecto poner en sus manos la tecnología más avanzada, a fin de equilibrar fuerzas.

Una vez realizada esta labor, es necesario reconocer que los Estados están incapacitados para comenzar a dictar leyes internas que se dirijan principalmente a la sanción de conductas bélicas, es necesario reconocer que el ciberespacio, como campo de desarrollo de actividades y la infoesfera como el cúmulo de las relaciones entre ciberciudadanos, merecen la atención de la comunidad internacional.

Este ejercicio debe ser total, debe contar con la participación de todos los Estados, ya que los sistemas y redes interconectadas al tener acceso garantizado, deben sujetarse a la voluntad general de la comunidad cibernética. Un solo actor fuera de sitio, puede devolver la paranoia y evitar un acto puro de integración necesario.

A fin de impedir las agresiones dentro de los sistemas, el robo de información y otras conductas antijurídicas será necesario eliminar el uso de armas cibernéticas y sancionar su desarrollo y aplicación, fortalecer lo sistemas y mantener un estrecha comunicación con todos los actores

La supervisión y vigilancia del ciberespacio debe ser delegada a uno o varios organismos superiores, como la Unión Internacional de Telecomunicaciones y algunos, cuya base sea garantizar la transparencia en el uso de ciberespacio,

el mantenimiento de la arquitectura y el estándar de lenguaje o protocolo existente, para que se aprovechen al máximo sus recursos.

Estos organismos internacionales, así como la Asamblea Permanente de la Organización de las Naciones Unidas pueden ser la autoridad superior en cuanto a la guerra cibernética y el aprovechamiento del ciberespacio, ya que al ingresar en el mismo se esta fuera de un Estado determinado, y cualquier acto antijurídico puede afectar a cualquier usuario.

Los Estados deben garantizar el libre acceso a los sistemas cibernéticos, y reconocer que la persona posee indefectiblemente los derechos humanos de información y la libre organización, manifestación de ideas, reunión, expresión, y otros nuevos que deben reconocerse como el intercambio de información, incluyendo la cultura y las ciencias.

El hombre es un ser social por naturaleza, es imposible limitar un derecho como estos mediante normas locales, ya que atentaría contra la misma esencia del ser. Si por ejemplo se sanciona una agresión por parte de un Estado en contra de otro, el posible castigo será ser desconectado un tiempo determinado, pero esto producirán afectaciones a la población civil, al sistema bancario financiero, a los sistemas como luz y agua; provocando de esta forma caos, paranoia, disturbios.

Los Estados deben asegurar el conocimiento del uso del ciberespacio a cualquier persona, es decir, que nadie en posibilidades de acceder se quede sin acceso por falta del conocimiento del sistema. Un pueblo educado es de mucho mejor ayuda que uno ignorante.

Como una medida especial de seguridad a fin de eliminar la guerra cibernética, es imperativo que los Estado que mantengan estrecha vigilancia de los sistemas, deben renunciar a ella y solo mantenerla en sistemas críticos propios, evitando la invasión o espionaje de sus homólogos.

Por ultimo, existen estados como Rusia y China que se han convertido en pioneros en el desarrollo de la guerra cibernética, en el caso del primero, es importante señalar que su estancamiento en la carrera armamentista y posterior caída, derivó en una necesidad de búsqueda de nuevas vías o métodos que le permitieran obtener una ventaja determinada sin necesidad de auxiliarse de la fuerza masiva, su situación es interesante ya que algunos autores sostienen que dada su experiencia en el campo, puede convertirse en el promotor de los acuerdos internacionales que se encaminen a la disminución en el uso de la guerra cibernética. Fortaleciendo su situación en el ámbito internacional, conservando su independencia de EUA y garantizando la participación de los países en subdesarrollo; aunque esta situación puede estar alejada de la realidad dado que Rusia a protagonizado los mayores ataques cibernéticos,

En cuanto a China, es de notarse el increíble crecimiento que ha presentado, muchas veces a costa de su entorno y su población, la violación de derechos humanos y el espionaje. De esta forma se ha allegado de los medios para comprender de una mejor forma las implicaciones de la guerra cibernética, potenciando su capacidad militar mediante el uso de sus millones de ciudadanos a manera de arsenal. Un caso notable es el de “La Gran Muralla de Fuego China”, que es un filtro de información y comunicaciones que impiden o censuran ciertos contenidos , así la población civil en China carece de acceso a información contraria al régimen oficial, por lo que se ven obligados a utilizar métodos diversos para lograr el acceso total al ciberespacio.

El sector privado, ejerce una gran influencia en el sistema internacional, ya que de el deriva principalmente el flujo de capitales; la economía integrada es más vulnerable a los caprichos de los dueños del dinero, comprenden una influencia externa al sistema, su poder no implica que formen parte del orden internacional como actores, o que sean reconocidos como sujetos, pero la fuerza que articulan es de tomarse en cuenta.

Los millones de personas que dependen de las corporaciones, o las bolsas del mundo que pueden caer con una simple transferencia de dinero, o una compra

súbita de cierta moneda, nos dan una idea del sector más afectado por estos grupos.

Existe convencimiento popular en cuanto a sus practicas salvajes, se valen del robo de información, la guerra psicológica, las comunicaciones, los medios masivos de difusión, para lograr su objetivo, todo parte de la cibernética, por ello la importancia que puede revestir el que este sector tenga la capacidad de hacer uso de los recursos de la guerra cibernética.

Las transnacionales también se ven interesadas en este tipo de enfrentamiento, ya que el avance tecnológico de muchos países como China, se debe en gran medida al espionaje industrial y militar, tareas de inteligencia y mercado negro de información.

Esta situación aunada a la dificultad de muchos Estados del mundo que no cuentan con los recursos necesarios para invertir en el desarrollo de ciencia y tecnología y de esta forma lograr un balance con respeto a lo demás, ha impulsado que los gobiernos contraten a las empresas privadas o asignen concesiones con respecto a áreas estratégicas del desarrollo estatal; agua, energía, alimentos, armamento, telecomunicaciones, esto con el pretexto de lograr más avance en poco tiempo, lo que se olvida es que los fines que buscan el estado y el sector privado son diametralmente opuestos, así se ponen en riesgo la estabilidad de todos los países.

La maquinaria del sector privado es algo difícil de contener y sobretodo en este mundo integrado con base en el capitalismo, comenzando con acuerdos internacionales que limiten la participación de estos sectores en el mantenimiento del ciberespacio, el desarrollo de armas digitales, bombardeo de publicidad, el trafico de bases de datos personales.

Así mismo, los organismos empresariales mundiales, deben encaminarse a la comprensión de que el ciberespacio es una puerta para el desarrollo mundial, y evitar pensar que se trata solo de un nuevo mercado. De esta forma la tendencia será guiada a una educación y conocimiento responsable de las

capacidades, fines y beneficios del ciberespacio, logrando un nuevo estatus de empresa social.

La participación de la sociedad civil tiene gran importancia, y se debe comprender dentro de esta, por excepción a todos aquellos usuarios que no representen a los estados ni al sector privado.

En principio, el acceso de los ciberciudadanos debe ser totalmente asequible, en cualquier lugar del globo; tiene especial importancia las multicitadas garantías de expresión e intimidad, ya que estas permiten el libre flujo de información, evitando la censura.

La intervención en asuntos públicos, tanto locales como internacionales y el libre intercambio de ideas debe ser confirmado por todos los países; es una realidad que la opinión publica internacional se ha convertido en un medio más de presión en contra de situaciones de desigualdad y crimen, principalmente en los países más desarrollados donde existe más respeto por estos derechos; aunque en los países en subdesarrollo también constituyen armas poderosas para captar la atención de la comunidad internacional.

Tal es el caso por ejemplo de el levantamiento del Ejercito Zapatista de Liberación Nacional, que realizó difusión en el ciberespacio, y logró de esta forma que los ojos del mundo, y visitadores de varios lugares del planeta garantizaran un cierto nivel de seguridad para el movimiento, de este modo se evito una mayor y sangrienta represión.

Ante este tipo de situaciones se puede mencionar la proliferación las cadenas de correo electrónico, comunidades políticas virtuales, redes de personas, foros de discusión, intercambio de archivos mediante sistemas P2P, web blogs; sin finalidad específica, personales, religiosos, comerciales. En ellos se establecen situaciones y se maneja información casi infinita, reducen el costo de las comunicaciones, y permiten la participación de las sociedades civiles en temas de discusión de suma importancia, pero se encuentran demasiado vigilados por las corporaciones y gobiernos que prestan dichos espacios, al nivel de condicionar la entrega de información confidencial para mantener acceso.

Como ya se ha apuntado es necesaria la vigilancia, pero también lo es mantener el respeto por el usuario y la información que vierte en el espacio cibernético. Para el caso, se hace deseable la aportación de cualquier usuario, para mantener la seguridad de todo el sistema. En cada servicio o pagina del Internet están clasificados por zonas y contenido, de este modo, los mismos usuarios pueden filtrar la información que se les presenta y denunciar la existencia de sitios ilegales.

En este tipo de situaciones , la mejor vigilancia es la del vecino, nada sucede en la red sin que alguien se de cuenta de ello; claro que la cautela es necesaria pero en niveles razonables, de lo contrario se corre el peligro de provocar paranoia en los usuarios, el desarrollar una vigilancia estatal o privada, provoca más problemas que respuestas, es risible creer que existen Estados que pretenden mantener una vigilancia total del sistema cibernético a fin de asegurar el orden, cuestiones que carecen de sustento tanto social como legal, de acuerdo a lo expuesto en el presenta trabajo, se consideran estos actos, violatorios de los derechos humanos en su totalidad.

En el caso de los organismos reguladores como la Administración de Nombres de Dominio y algunos otros como la Internet Society, la función que realizan al mantener los estándares de operación del ciberespacio y pugnar por el crecimiento, difusión y acceso al mismo, es lo que hace posible el funcionamiento del sistema, son necesarios mantenerlos en operación a fin de evitar colapsos en las redes.

La sociedad civil ahora presenta una nueva interrogante ante el fenómeno de la guerra cibernética, ya que puede efectivamente tomar partido en las hostilidades en contra de cualquier Estado sin pertenecer a alguno de los combatientes, de forma directa con ataques mediante el uso de armas digitales o de forma indirecta, por medio de la guerra psicológica, la manipulación de la opinión publica internacional.

En este caso, cada Estado será responsable de sus ciudadanos, y hay que comprenden el termino utilizado, si bien los actos que realizan en pro de la guerra cibernética es con el estatus de ciberciudadano, las consecuencias se

dejan sentir en el mundo real. Para este caso, será imperativo la adecuación de los tipos penales; los tratados sobre cooperación y extradición.

Sería imposible pensar en un ciberespacio igualitario sin tomar en cuenta preponderantemente a los usuarios civiles como personas singulares y las organizaciones antes citadas, ya que prácticamente el contenido del ciberespacio esta construido en las redes que estos crean, inclusive ahora se tienen redes comunitarias, agrupaciones cibernéticas reunidas gracias a los beneficios del espacio virtual, que permiten la participación interactiva y directa de personas en discusiones encaminadas al mejoramiento de la sociedad, tanto de la infoesfera como del mundo tangible. Cualquier esfuerzo por lograr una mejor convivencia en línea deberá ser tomada en consenso con estas partes.

4.5 Descripción de Enfrentamientos Reales en el Ciberespacio

Si bien es cierto la guerra cibernética es apenas una simiente, ello no implica que desde hace algunos años se hayan comenzado a realizar incursiones en los sistemas cibernéticos de Estados agredidos, de los cuales ha derivado el robo de información, espionaje, saturación y colapso de sistemas, e inclusive, aunque sin comprobar, ataques exitosos a infraestructura crítica.

Dada esta situación, en adelante se hace referencia a algunos de estas avanzadas, en razón de que será en pocos años que seremos testigos de la primera guerra cibernética internacional.

-El 20 de julio de 2007, derivado de la situación particular de la provincia Osetia del sur, perteneciente al país Georgia, y el movimiento separatista apoyado por el gobierno Ruso, diversos hackers principalmente de este ultimo país realizaron invasiones a los sistemas de Georgia, saturando servidores y realizando propaganda política en favor de la separación de ambas regiones.

Es la primera vez que un país combina la guerra cibernética con incursiones de guerra convencional, aunque las consecuencias fueron limitadas, estos ejercicios se están haciendo cada vez más comunes a medida que se amplían las redes y avanza la tecnología.[62]

-Una rencilla por el retiro de un monumento soviético ubicado en Tallin, capital de Estonia, provocó la ira del vecino estado Rusia, mismo que tomo el hecho como un ataque directo

El 27 de abril de 2007, comenzó la incursión cibernética más grande de la historia, en contra del que se conoce como el país más conectado del mundo. Al principio se saturaron las paginas de los principales periódicos de Estonia, lo que provoco fallas en los principales servidores de el país, situación que duró con altas y bajas n el servicio.

El 2 de mayo de 2007, la situación empeoró, miles de solicitudes provenientes de países de Asia, Sudamérica y Medio Oriente, provocaron definitivamente el colapso de la red del periódico más importante de Estonia., el gobierno de Estonia tuvo que cortar el trafico internacional hacia el sitio del rotativo.

A las 11 de la noche del 9 de mayo de 2007, más de un millón de computadoras diseminadas por todo el mundo estaban realizando solicitudes de acceso a sitios Web de Estonia, se saturaba la capacidad de las redes estonias para atender dichas peticiones de acceso.

El gobierno de Estonia, tuvo que recurrir a algunos de los operadores extraoficiales que tienen el poder para cortar el flujo de información del ciberespacio en una región o en todo el mundo, estas personas autorizaron, conjuntamente con Proveedores de Servicios de todo el planeta, el bloqueo de las redes que estaba atacando los sitios de Estonia, logrando para mediados de mayo de 2007 el restablecimiento del sistema con las siguientes consecuencias derivadas de la agresión:

Se saturaron las paginas del gobierno de Estonia, mediante el uso de ataques ping, miles de peticiones de acceso a diversas paginas y redes, saturan la capacidad de respuesta de las mismas, provocando su colapso.

Los números de emergencia, incluyendo bomberos quedaron fuera de servicio.

Las comunicaciones celulares del mismo modo se inutilizaron, afectando la tecnología conocida en México como Nipper, que permite el pago y contratación de servicios vía celular.

---

[62] EL PAIS, "Guerra en el Caucaso. Georgia sufre la Guerra Cibernética." , Nueva York 14 de Agosto de 2008
http://www.elpais.com/

Se realizaron robos y transferencia de dinero en línea

Cajeros automáticos y acceso satelital a Internet fue inservible

Al cortar el flujo de información del ciberespacio, Estonia se aisló prácticamente del resto del mundo.

El ataque se realizó mediante el uso de varias *botnets* o redes de computadoras infiltradas y utilizadas como zombis, que realizaron un tipo de barrido de sistemas críticos conocido como DDOS por sus siglas en ingles, Distributed Denial of Service, logrando saturar la red de estonia, impidiendo su uso y operación correcta; lo increíble es la capacidad para manejar tantos ordenadores con precisión y coordinación absoluta.[63]

-Durante la Guerra de Israel contra Líbano en 2006, el grupo conocido como Hezbollah demostró su capacidad para abrir otros campos de batalla; al unísono con la respuesta a los bombardeos de Beirut, se realizaron acciones de guerra convencional y guerra cibernética, dirigidas estas ultimás en contra de las paginas del gobierno Israelita, así como contra aliados como Estados Unidos, implicando sobre todo, invasión a sistemas militare y robo de información. [64]

-Durante el año 2003, se lleva a cabo la operación Titan Ram, donde hackers chinos se encargan de infectar y robar información y bases de datos de las computadoras centrales de la empresa armamentista Lockheed Martín, productora de misiles y aviones a gran escala para el gobierno Estadounidense, así como la NASA y otro sitios.

En 1999, tuvo lugar la llamada operación Moonlight Maze, una operación en contra de Estados Unidos, por dos frentes, Rusia por un lado infiltra las redes del Pentágono y la NASA, robando enormes cantidades de datos militares, entre ellos, información sobre los sistemas de guía de misiles. China por otro lado, ataca inutilizado diversos sitios Web de Estados Unidos en respuesta a la el bombardeo de la embajada china en Belgrado.[65]

---

[63] DAVIS, Joshua, *"Guerra en la Red"*, en Selecciones, Ed. Reader's Digest México S. A. de C.V. México, Agoto 2008, Págs. 96-106

[64] CNN, "Hezbollah y la Guerra Cibernetica" , Estaos Unidos de América, 06 de Julio de 2008 http://edition.cnn.com

[65] GRECKO, Témoris, *"Ciberguerras. Terror en la Red"*, en QUO, Ed. Expansión S.A. de C.V. y Hachette Filipacchi S.A. México, No. 124 Febrero 2008, Págs. 91-99

CONCLUSIONES

1.- Atender al principio de mutabilidad y la capacidad de adaptación de las ciencias sociales en relación con la tecnología es un paso necesario para hacer del Derecho, una mejor forma de orden y estructura social transdiciplinaria e integradora del conocimiento.

2.- La red mundial de Internet es un hecho jurídico que de forma consensuada y fortuita produce una variación en la esfera de todo aquel que tenga acceso al mismo, y mantiene su independencia, autorregulación y gobernanza descentralizada.

3.- La libre asociación global y la libertad de acceso conforman lo dos principios básicos del ciberespacio, gracias a su reconocimiento la infoesfera es una realidad, logrando una equivalencia con los derechos fundamentales de información, comunicación y expresión.

4.- El concepto del ciberespacio es la zona artificial creada por la interconexión de las redes mundiales de comunicación e información.

5.- La guerra es un medio de autotutela colectiva, implica un acto antijurídico y regulado por el Derecho Internacional, rebasa el orden normativo interno de los Estados.

6.- La cibernética es una ciencia totalizadora, tiende a lograr control sobre cada uno de los sistemas que estudia, para las ciencia sociales y el Derecho su uso busca mejorar la velocidad de adaptación y una mejor correspondencia con la conducta humana de forma tal que la norma posea mayor eficacia con la garantía de realimentación que permita su perfeccionamiento constante.

7.- El estudio de la guerra cibernética se encuadra en el Ius in Bello ya que se refiere aún nuevo medio de agresión que necesariamente debe ser limitado por el Derecho Internacional con miras a prevención.

8.- La guerra cibernética es una realidad reconocida, sus efectos se dejan sentir en los países desarrollados principalmente y debido al porcentaje de conexión de sus sistemas al ciberespacio; los ejércitos del mundo poseen áreas determinadas para su desarrollo por lo que los esfuerzos para estructurar un sistema de control democrático que permita a los usuarios en general las libertades fundamentales así como la seguridad en cualquier relación que establezcan aún no se cristalizan.

9.- La guerra cibernética es el acto por medio del cual Estados soberanos en conflicto pretenden la imposición reciproca de intereses mediante el uso las herramientas electrónicas e informáticas, dirigidas a la supresión de los sistemas de control enemigos, al tiempo en que se sostienen los propios.

10.- Se impulsa la aceptación de un concepto de soberanía de la comunidad internacional, por tanto la adecuación en el alcance del concepto contemporáneo es inaplazable.

11.- En cuanto al ámbito de validez material la guerra cibernética se rige por el Derecho Internacional público dada la naturaleza global que incumbe de manera importante a la seguridad de los Estados.

12.- En el ámbito personal el sujeto activo será cualquier Estado con acceso al ciberespacio y que mediante diversos medios haga uso de la agresión en contra de otro, el sujeto pasivo será cualquier Estado que sufra las consecuencias de la agresión inclusive cuando los afectados del Estado agredido carezcan de acceso al sistema.

13.- En el ámbito temporal la vigencia del orden internacional que regule la guerra cibernética debe tener un inicio pero nunca un fin, ya que los principios expuestos poseen la característica de mutabilidad haciendo factible la adecuación sin rezago.

14.- El ámbito espacial existe pero carece de territorio, el orden jurídico debe abarcar a cada uno de los usuarios del ciberespacio; cada acceso al sistema y cualquier punto del mismo en todas sus interconexiones poseen dos ámbitos definidos: uno global que incumbe a la comunidad internacional derivado de las agresiones cometidas y uno local para la vigilancia y respuesta física a las amenazas.

15.- Es necesaria una convención internacional que garantice el respeto y cumplimiento de los principios propuestos ya que la fuerza vinculatoria es necesaria en los acuerdos jurídicos tanto para garantizar derechos como para hacer cumplir obligaciones. La costumbre o las declaraciones son insuficientes.

16.- El ciberespacio es res communis, por tanto las incursiones bélicas afectan a todos los usuarios de sistema y dan nacimiento a la responsabilidad internacional por su uso.

17.- La eliminación de la brecha tecnológica es urgente, por lo que es imperativo para la comunidad internacional lograr la homologación en los sistemas de información y comunicación.

18.- La competencia reconocida para la guerra cibernética es principalmente el ciberespacio y debe de ser facultada de la Organización de Naciones Unidas y de la Corte Internacional de Justicia atender la problemática derivada de sus uso.

19.- La seguridad puede lograrse mediante el ajuste adecuado de programas criptográficos y firmas electrónicas para la identificación de usuarios; la vigilancia debe estar dirigida a lograr un sistema global ciberciudadano en el que participen todos los usuarios; la intimidad no debe ser violada bajo ningún motivo pero deben fijarse identificaciones de cada proveedor de servicios y vigilar el contenido que fluye en red, más no filtrarlo. Tomar partido por la

liberalización o por la seguridad total es un error, se pretende optar por la educación y cultura en el cuidado del ciberespacio.

20.- Es de vital importancia reconocer la gobernanza en el ciberespacio como una institución cuyo objetivo sea lograr la participación de Estados, corporaciones, organizaciones civiles, organismos no gubernamentales y ciberciudadanos, evitando el uso de redes estatales regionales que pretendan participar de los beneficios, pero eviten integrarse al orden jurídico propuesto.

21.- Aunque la guerra, desde el comienzo de la civilización ha estado unida la ser humano, el Derecho debe velar por su eliminación y erradicar justificaciones para el uso de la fuerza o doctrinas sin sentido como la de Guerra Justa y Guerra Preventiva.

FUENTES

LIBROS

BASAVE FERNÁNDEZ DEL VALLE, Agustín
Filosofía del Derecho Internacional
Ed. IIJ UNAM Segunda Edición
México 1989

BECERRA RAMÍREZ, Manuel
Derecho Internacional Publico
Ed. IIJ UNAM
México 1991

BECERRA RAMÍREZ, Manuel Et. Al.
Aspectos Juridico Políticos de la Guerra en Irak
Ed. IIJ UNAM
México 2005

BIDWELL, Shelford
World War 3; A Terrifying Projection Founded On Today's Facts
Ed. Cambridge
UK. 1980

DOMÍNGUEZ MARTÍNEZ, Jorge Alfredo.
Derecho Civil. Parte General. Personas, Cosas, Negocio Juridico e Invalidez
Ed. Porrúa. 8ª Edición
México 2000

Enciclopedia Jurídica Latinoamericana Tomo V
Rubinzal-Culzoni Editores
Argentina 2007

FERNÁNDEZ RODRÍGUEZ, José Julio.
Lo Publico y lo Privado en Internet. Intimidad y Libertad de Expresión en la Red
Ed. IIJ UNAM
México 2005

GARCÍA BARRERA, Myrna Elia
Derecho de las Nuevas Tecnologías
Ed. IIJ UNAM
México 2008

GARCÍA MAYNEZ, Eduardo.
Introducción al Estudio del Derecho
Ed. Porrua 58ª Edicion
México, 2005

GOMEZ LARA, Cipriano
Teoria General del Proceso
Ed. Oxford 10ª Ed.
México 2004

GORDON, E.
Electronic Warfare: Element of Strategy an Multiplier of Combat Power
Ed. Pergamon Press
New York 1981

GRIFFIN, David
Developments in E-Government: A Critical Analisis
Ed. IOS
Amsterdam 2007

HANT
War, Morality and Autonomy: An Investigation in Just War Theory
Ed. Ashgate
Inglaterra 2004

HELLER, Hermann
La Soberanía
Ed. UNAM y FCE 2ª ED
MEXICO, 1995

KENETH EIMAR HIMMA
Internet Security: Hacking, Counter Hacking and Society
Ed. Jones and Bartlett
E.U. 2007

KINDENLAN, Alfredo
La Próxima Guerra
Ed. M. Aguilar 3° Edición
Madrid, España

LIVAS, Javier
Cibernetica, Estado y Derecho.
Ed. Gernika
México 1988

LÓPEZ MÁRTINEZ, Mario Dir
Enciclopedia de Paz y Conflictos
Ed. Universidad de Granada
España 2004

MAQUIAVELO , Nicolás
El Principe
Ed. Multimedios
MEXICO 1999

MARTOS RUBIO, Ana
Internet
Ed. Anaya Multimedia
Madrid España 2007

MÉNDEZ SILVA, Ricardo Et. Al.
Derecho de los Conflictos Armados
Ed. IIJ UNAM
México 2003

MEZA SALAZAR , Martha Alicia
Estado Telemático y Teoría del Estado
S/E
México 2006

OVALLE FAVELA, Jose
Teoría General del Proceso
Ed. Oxfor, 4º Ed.
Mexico 1998

RÍOS ESTAVILLO, Juan José
Derecho e Informática en México
Ed. IIJ UNAM
México 1997

ROJAS AMANDI, Víctor Manuel
El Uso de Internet en el Derecho
Ed. Oxford University Press
México 2000

ROSSEAU, Jean-Jacques,
El Contrato Social
Ed. Distribuciones Mateos S. A.
Madrid, España 1993

SENIOR, Alberto F.
Filosofía del Derecho
S.E.,
MEXICO 2002

SORRELS, William T
Guerra Cibernética 2.0: Mitos; Misterios y Realidades
Ed. AFCEA International Press
Argentina 2007

TÉLLEZ VALDEZ, Julio .
Derecho Informático
Ed. IIJ UNAM

México 1991

TUNKIN, G.I.
El Derecho y la Fuerza en el Sistema Internacional
Ed. IIJ UNAM
México 1989

VERSTRYNGE ROJAS, Jorge
Una Sociedad para la Guerra; (Los Efectos de la Guerra en la Sociedad Industrial)
Ed. Centro de Investigaciones Sociológicas.
Madrid, 1979

WALZER, Michael
Reflexiones Sobre la Guerra
S/E
Carmen castell y Claudia Casanova, Trad.
México 2004

REVISTAS

AARON, Raymond, *"Paz y Guerra entre las Naciones"*, Revista de Occidente, 2ª Edición, Madrid, España, 1963, Págs. 101-126

BOTERO BERNAL, Andrés. *"Los Retos del Jurista Internacionalista en la Contemporaneidad",* Anuario Mexicano de derecho Internacional Vol IV 2004 pp. 251-288

CANO GARZON, Octavio Augusto, *"La Doctrina Bush de la Guerra Preventiva. ¿Evolución del Ius Ad Bellum o vuelta al Medioevo?,* Ed. Universidad Pontifica Bolivariana, Medellín , Colombia, Vol. 36, No. 105. Julio – Diciembre 2006

DAVIS, Joshua, *"Guerra en la Red"*, en Selecciones, Ed. Reader's Digest México S. A. de C.V. México, Agoto 2008, Págs. 96-106

GRECKO, Témoris, *"Ciberguerras. Terror en la Red"*, en QUO, Ed. Expansión S.A. de C.V. y Hachette Filipacchi S.A. México, No. 124 Febrero 2008, Págs. 91-99

LOPEZ, Claudio C. *"La Guerra Informática"*, en Boletín del Centro Naval, S. E. , Argentina, número 817, Mayo – Agosto 2007, pags. 221

"Guerra en el Caucaso. Georgia sufre la Guerra Cibernética." , El País, Nueva York 14 de Agosto de 2008

"Hezbollah y la Guerra Cibernetica" , CNN, Estados Unidos de América, 06 de Julio de 2008

LEYES Y REGLAMENTOS

CÓDIGO DE COMERCIO
Publicación Diario Oficial de la Federación, 15 de septiembre de 1889
Inicio Vigencia Primero de enero de 1890

CÓDIGO FISCAL DE LA FEDERACIÓN
Publicación Diario Oficial de la Federación 31 de diciembre de 1981
Inicio Vigencia Primero de enero de 1983

CÓDIGO PENAL FEDERAL
Publicación Diario Oficial de la Federación 14 de agosto 1931
Inicio Vigencia 17 de septiembre 1931

LEY FEDERAL DE TELECOMUNICACIONES
Publicación Diario Oficial de la Federación 7 de junio de 1995.
Inicio Vigencia 8 de junio de 1995

REGLAMENTO DE LA COMISIÓN FEDERAL DE TELECOMUNICACIONES
Publicación Diario Oficial de la Federación 2 de enero de 2006
Inicio Vigencia 5 de enero de 2006

TRATADOS INTERNACIONES

Convención para la Adaptación de los Principios de la Convención de Ginebra a la Guerra Marítima, 22 de agosto de 1864

Convención relativa al Rompimiento de Hostilidades, La Haya el 18 de octubre de 1907

Convención Concerniente a las Leyes y Usos de la Guerra Terrestre
el 18 e octubre de 1907

Pacto Briand – Kellog.- París 27 de agosto de 1928

Carta de la Organización de las Naciones Unidas, San Francisco, Estados Unidos, 26 de Junio de 1945

Convención de Ginebra , 12 de agosto 1949,

Convención Sobre la Protección de los Bienes culturales en Caso de Conflicto Armado.- La Haya, 14 de mayo de 1954

Resolución No. 2131 Declaración de la Asamblea General De la Organización de las Naciones Unidas sobre la Inadmisibilidad de la Intervención en los Asuntos Internos de los estados y Protección de su Independencia y Soberanía, 21 de diciembre de 1965

Resolución 2625 Declaración de la Asamblea General de la Organización de las Naciones Unidas sobre los Principios de Derecho Internacional referentes a las

Relaciones de Amistad y a la Cooperación entre los Estados de conformidad con la Carta de las Naciones Unidas; de 24 de octubre de 1970

Resolución 3314. Definición de la Agresión Nueva York, Estados Unidos de América. Vigésimo Noveno Periodo de Sesiones. Suplemento No. 19. 2319ª Sesión Plenaria, 14 de diciembre 1974

Resolución No. 42/22 Declaración de la Asamblea General de la Organización de las Naciones Unidas sobre el Mejoramiento de la Eficacia del Principio de la Abstención de la Amenaza o de la Utilización de la Fuerza en las Relaciones Internacionales, 18 de noviembre de 1987

Resolución No. 3314 Declaración de la Asamblea General de la Organización de las Naciones Unidas sobre la Definición de Agresión, 14 de diciembre de 1974

Resolución No. 34/88 Declaración de la Asamblea General de la Organización de las Naciones Unidas sobre la Cooperación Internacional para el Desarme, 11 de diciembre de 1979

Resolución No. 37/10 Declaración de Manila sobre el Arreglo Pacífico de Controversias Internacionales, 15 de noviembre de 1982

Declaración de Principios de Ginebra Cumbre Mundial sobre la Sociedad de la Información, Diciembre 2005

PAGINAS DE INTERNET

http://edition.cnn.com

http://www.apc.org

http://www.elpais.com/

http://www.itu.int/net/about/legal-es.aspx

http://www.itu.int./wsis/index-es.thml

http://www.oecd.org

http://www.uncitral.org

http://www.wipo.int/about-wipo/es/what/