UNIVERSIDAD MAYOR DE SAN ANDRÉS

FACULTAD DE DERECHO Y CIENCIAS POLÍTICAS
CARRERA DE DERECHO

TESIS DE GRADO
"TERRORISMO NFORMÁTICO Y SU PERSPECTIVA JURIDICA"

POSTULANTE: ERICK RENJEL VELÁSQUEZ

TUTOR: Dr. MARCELO FERNANDEZ IRAOLA

LA PAZ - BOLIVIA

I N D I C E

INTRODUCCIÓN 1

1. PLANTEAMIENTO DEL PROBLEMA 5
1.1. PROBLEMATIZACIÓN 5

2. DELIMITACIÓN 6
2.1. TEMÁTICA 6
2.2. TEMPORAL 9
2.3. ESPACIAL 9

3. JUSTIFICACIÓN 9

4. OBJETIVOS 10
4.1. OBJETIVOS GENERALES 10
4.2. OBJETIVOS ESPECÍFICOS 11

5. HIPÓTESIS 12

6. VARIABLES 12
6.1. INDEPENDIENTE 12
6.2. DEPENDIENTES 12

7. METODOLOGÍA 13

8. TÉCNICAS 15

CAPITULO I
EL TERRORISMO

1.1. ANTECEDENTES 16
1.1.1 CULTURAS PRIMITIVAS 17
1.1.2 GRECIA Y ROMA 17
1.1.3 DESPOTISMO ILUSTRADO (SIGLO XVIII)..... 19
1.1.4 TERRORISMO CONTEMPORANEO (SIGLO XIX – XX) 20
1.1.5 NEOTERRORISMO 21

1.2. CONCEPTO Y DEFINICION 21

1.3. PERFIL DEL TERRORISTA 23

1.4. TIPOS DE TERRORISTAS 24

1.4.1. TERRORISTAS CLÁSICOS 24

1.4.2. TERRORISTAS SUICIDAS 24
1.5. OBJETIVOS 25
1.6. CARACTERISTICAS 25
1.7. MEDIOS PARA COMBATIRLO 26
1.7.1. NO HOME 26
1.7.2. NO TRAINING 27
1.7.3. NO FINANCE 27
1.7.4. NO MORAL GROUNDS 28
1.7.5. OTROS MEDIOS 29
1.8. ATAQUES TERRORISTAS A ESTADOS UNIDOS (11 DE SEPTIEMBRE) 29
1.8.1. ORDEN MILITAR SOBRE "DETENCIÓN, TRATO Y JUICIO DE CIERTOS NO CIUDADANOS EN LA GUERRA CONTRA EL TERRORISMO" 31
1.9. TERRORISMO EN SUDAMERICA 36

CAPITULO II
CLASIFICACION DEL TERRORISMO

2.1. DE ACUERDO AL OBJETIVO 42
2.1.1. SEGÚN EL ALCANCE DEL OBJETIVO 42
2.1.1.1. TERRORISMO GLOBAL 42
2.1.1.1.1. Al Qaida 43
2.1.1.1.2. Baader - Meinhof 44
2.1.1.2. TERRORISMO FOCAL 45
2.1.1.2.1. Hamas 46
2.1.1.2.2. Hezbola 47
2.1.2. SEGÚN EL TIPO DE BLANCOS 47
2.1.2.1. BLANCOS INSIGNIA 47
2.1.2.2. BLANCOS REGIONALES 48
2.2. DE ACUERDO AL MEDIO UTILIZADO 48
2.2.1. TERRORISMO BIOLOGICO (BIOTERRORISMO) 48
2.2.2. TERRORISMO INFORMATICO (CIBERTERRORISMO) 51

2.3. TERRORISMO DE ESTADO ……. 52

CAPITULO III
CONTEXTO INTERNACIONAL
EN LA LUCHA CONTRA EL TERRORISMO

3.1. ORGANISMOS INTERNACIONALES …… 54

3.1.1. ORGANIZACIÓN DE LAS NACIONES UNIDAS **(ONU)** …… 54

3.1.1.1. RESOLUCION 1368 de 12 de septiembre de 2001 Condena de los ataques terroristas perpetrados en los EEUU. …… 56

3.1.1.2. RESOLUCIÓN 1373 de 28 de Septiembre de 2001 Consejo de Seguridad - Organización de las Naciones Unidas sobre Terrorismo (Nuevas Medidas para combatir al terrorismo) ……. 57

3.1.1.3. RESOLUCIÓN 1377 de 12 de Noviembre de 2001 Declaración Adjunta sobre los esfuerzos mundiales para combatir al terrorismo …… 58

3.1.1.4. RESOLUCIÓN 1456 de de 20 de Enero de 2003 - Decide Aporbar la Resolución adjunta sobre la de la lucha contra el terrorismo …… 59

3.1.1.5. CONVENIOS INTERNACIONALES Nuevas medidas para combatir al terrorismo …… 60

3.1.2. ORGANIZACIÓN DE LOS ESTADOS AMERICANOS

(OEA) …… 62

3.1.2.1. CONVENCIÓN INTERAMERICANA CONTRA EL TERRORISMO (Aprobada en la primera sesión plenaria celebrada el 3 de junio de 2002 …… 62

3.1.2.2. CONVENCION PARA PREVENIR Y SANCIONAR LOS ACTOS DE

TERRORISMO CONFIGURADOS EN DELITOS CONTRA LAS PERSONAS Y LA EXTORSIÓN CONEXA CUANDO ESTOS TENGAN TRASCENDENCIA INTERNACIONAL (Suscrita en el Tercer Periodo Extraordinario de Sesiones de la Asamblea General de 2 de febrero de 1971) 63

3.2. CONVENIOS INTERNACIONALES 65

3.2.1. CONVENIO DE GINEBRA PARA LA PREVENCION Y REPRESION DEL TERRORISMO DE 1937 65

3.2.2. CONVENCION EUROPEA PARA LA REPRESION DEL TERRORISMO DE 1977 65

3.2.3. CONVENCION DE LA ORGANIZACIÓN DE LA UNIDAD AFRICANA SOBRE LA PREVENCION Y LUCHA CONTRA EL TERRORISMO, DE 1999 66

3.2.4. CONVENCION DE LA ORGANIZACIÓN DE LA CONFERENCIA ISLÁMICA SOBRE LA LUCHA CONTRA EL TERRORISMO INTERNACIONAL, DE 1999 67

CAPITULO IV
INTERNET

4.1. ANTECEDENTES 70

4.1.1. PRIMER PERIODO: 1957 - 1970 (NACIMIENTO) 71

4.1.2. SEGUNDO PERIODO: 1970 - 1990 (DEL EJÉRCITO A LA UNIVERSIDAD) 72

4.1.3. TERCER PERIODO: 1990 - 1995 (EXPANSION) 73

4.1.4. CUARTO PERIODO: 1996 – 2004 (MULTIMEDIA – CIENTOS DE MILLONES DE USUARIOS) 74

4.2. CONCEPTO 75

4.3. FUNCIONAMIENTO 76

4.4. CONEXIÓN 77

4.5. UTILIDADES 77

4.5.1. BUSQUEDA DE INFORMACION 78
4.5.2. CHAT 78
4.5.3. VIDEOCONFERENCIA 79
4.5.4. CORREO ELECTRONICO 79

CAPITULO V
DELINCUENCIA INFORMATICA

5.1. EL DELITO 81

5.2. DELITO INFORMÁTICO 83

5.2.1. BIEN JURIDICO PROTEGIDO 85
5.2.2. ELEMENTO OBJETIVO 85
5.2.3. ELEMENTO SUBJETIVO 86
5.2.4. SUJETO ACTIVO 86
5.2.5. SUJETO PASIVO 87
5.2.6. CLASIFICACION DE LOS DELITOS INFORMATICOS 87

5.2.6.1. FRAUDES COMETIDOS MEDIANTE MANIPULACION DE COMPUTADORAS 87

5.2.6.1.1. Manipulación de Datos de Entrada..... 87

5.2.6.1.2. Manipulación de Programas 88

5.2.6.1.3. Manipulación de Datos de Salida 89

5.2.6.1.4. Manipulación Informática aprovechando Repeticiones Automáticas de los Procesos de Cómputo 89

5.2.6.1.5. Falsificaciones Informáticas ... 90

5.2.6.2. DAÑOS O MODIFICACIONES DE PROGRAMAS O DATOS COMPUTARIZADOS 90

5.2.6.2.1. Sabotaje Informático 90

5.2.6.3. ACCESO NO AUTORIZADO A SERVICIOS Y SISTEMAS INFORMÁTICOS 91

5.2.6.3.1. Piratas Informáticos 91

5.2.6.3.2. Reproducción Desautorizada de Programas Informáticos con Protección legal ……. 92

5.2.7. EL DELITO INFORMATICO EN LA LEGISLACIÓN NACIONAL …… 93

5.2.8. EL DELITO INFORMATICO EN LA LEGISLACIÓN INTERNACIONAL …… 95

5.2.8.1. ESTADOS UNIDOS …… 95
5.2.8.2. ALEMANIA …… 97
5.2.8.3. AUSTRIA …… 97
5.2.8.4. GRAN BRETAÑA …… 98
5.2.8.5. HOLANDA …… 98
5.2.8.6. FRANCIA …….. 99
5.2.8.7. ESPAÑA …… 100
5.2.8.8. CHILE …… 101

5.3. HACKERS …… 102

5.3.1. CRONOLOGIA DE LOS HECHOS MAS DESTACADOS 104

5.4. CRACKERS …… 107

5.5. PHRACKERS …… 109

5.6. LAMERS …… 110

CAPITULO VI
TERRORISMO INFORMATICO
(CIBERTERRORISMO – CYBERTERRORISM)

6.1. ANTECEDENTES …… 111

6.2. CONCEPTO …… 112

6.3. CARACTERÍSTICAS …… 114

6.3.1. ASIMETRÍA POLÍTICA - POLITICA ESTRATEGICA … 115
6.3.2. NUEVO CAMPO DE BATALLA (CIBERWAR) …… 116
6.3.3. BAJOS RECURSOS Y ALTO RIESGO …… 117
6.3.4. DIFÍCIL LOCALIZACIÓN …… 117
6.3.5. PLATAFORMA CIBERNÉTICA …… 118

6.4. FORMAS DE ATAQUE …… 119

6.4.1. HIGH TECH (ALTA TECNOLOGÍA) …… 121

6.4.1.1. INTERRUPCION 121
6.4.1.2. INTERCEPCIÓN 122
6.4.1.3. MODIFICACIÓN 122
6.4.1.4. FABRICACIÓN 123

6.4.1.4.1. Ataques Pasivos 123
6.4.1.4.2. Ataques Activos 124

A) Suplantación de Identidad 124
B) Reactuación 125
C) Modificación de Mensajes... 125
D) Degradación Fraudulenta
del Servicio 126

6.4.1.5. SPOOFING (Envio de Señales Falsas)..... 126
6.4.1.6. ESTEGANOGRAFIA 127
6.4.1.7. DoS (Ataques de Negación de Servicio)..... 128
6.4.1.8. PISHING (Obtención de Información
Mediante el Dolo) 128

6.4.2. LOW TECH (BAJA TECNOLOGÍA) 129

6.5. TIPOS DE ARMAMENTO INFORMATICO 131

6.5.1. ARMAS LOGICAS 131

6.5.1.1. VIRUS INFORMATICOS 131
6.5.1.2. BOMBAS LOGICAS 133
6.5.1.3. CABALLOS DE TROYA 135

6.5.2. ARMAS DE PULSO ELECTROMAGNÉTICO 136
6.5.3. PROGRAMAS FIRMWARE 137

6.6. TIPOS DE ATAQUE 137

6.7. ATAQUES IDENTIFICADOS 139

6.8. MEDIOS PARA LA LUCHA CONTRA EL TERRORISMO INFORMATICO 143

6.8.1. LOGICOS 143

6.8.1.1. CARNIVORO 145
6.8.1.2. ECHELON Y ENFOPOL 148

6.8.2. HUMANOS 150

CAPITULO VII

ANÁLISIS JURÍDICO DEL TERRORISMO INFORMÁTICO

7.1. UBICACIÓN JURÍDICA 152
7.1.1. DENTRO DEL DERECHO 152
7.1.2. DENTRO DEL DERECHO INFORMÁTICO 154
7.2. LEGISLACIÓN BOLIVIANA 154
7.2.1. EN EL FINANCIAMIENTO 157
7.2.2. EN LA ORGANIZACIÓN 158
7.2.3. POR LOS TIPOS DE ATENTADO 160
7.2.4. RATIFICACION Y ADHESIÓN A CONVENIOS Y PROTOCOLOS INTERNACIONALES REALIZADOS POR BOLIVIA 164
7.3. DERECHO COMPARADO 169
7.3.1. EE.UU. 169
7.3.2. ESPAÑA 172
7.3.3. GRAN BRETAÑA 173
7.3.4. ITALIA 175
7.3.5. SINGAPUR 176
7.3.6. SUDAFRICA 177

CONCLUSIONES 180
RECOMENDACIONES 181
BIBLIOGRAFIA 183
ANEXOS
..... 189

INTRODUCCION

CONSIDERACIONES GENERALES

Si bien el terrorismo, no es una práctica nueva, ahora ha encontrado con la aparición de nuevas tecnologías, un nuevo medio para crear pánico y zozobra en la población.

La aparición de terroristas que emplean medios informáticos para conseguir atemorizar, destruir y causar miedo, crece cada día; con el riesgo de penetrar en sistemas informáticos de uso ciudadano, militar, policial, e inclusive de seguridad nacional en todos los países incluido el nuestro.

A consecuencia, del desarrollo de la Informática, y el mal empleo de la misma, se puede producir un ataque terrorista, que provoque la destrucción de forma virtual a través de la red de redes (Internet), utilizando de tal forma medios informáticos, donde no es necesaria la presencia física del terrorista. Situación que hace más complejo el tema ya que la autoría y ubicación del delincuente se hace más complicada, debiendo por lo tanto desarrollarse un estudio sobre el terrorismo informático.

Los Ordenadores controlan de forma automática muchos procesos: control de aguas, reparto del fluido eléctrico, conmutación de una central telefónica, control de tráfico aéreo, etc. Situación que es aprovechada por los Ciberterroristas, quienes ingresando a los sistemas informáticos que controlan equipos electrónicos de los cuales depende el funcionamiento de los servicios mencionados; logran colapsarlos y provocar daños materiales, e inclusive la muerte de muchas personas.

Por lo que el Ciberterrorismo se convierte en un problema que no solo podría causar destrucción en infraestructuras y vidas humanas a nivel mundial y dentro de países desarrollados, sino que también afectaría a nuestro país, por el fácil acceso a los sistemas informáticos de control que utiliza el gobierno; ya que no existe seguridad ni protección lógica y legal, lo que ocasionaría que Bolivia se convierta inclusive en una Plataforma Cibernética.

Si bien el ataque se produce en el ciberespacio, debe tener un punto físico de origen, donde el terrorista utilizando medios informáticos (la computadora) e introducido en una red de control del sistema informático al que se quiere atacar; empieza su misión en deterioro del objetivo.

El ataque podría originarse desde diferentes sitios geográficos, utilizando el ciberespacio como canal de ejecución de objetivo. Sin embargo, la difícil localización del ataque terrorista, hace que no se pueda establecer con precisión las coordenadas de origen, ni tampoco la futura actuación terrorista, por lo que el control solo se puede establecer en base a direcciones IPS de computadora, que no son cien por ciento seguras, pero ayudan a la localización.

Tomando en cuenta el alcance mundial que el terrorismo informático a logrado dentro de los últimos años, y la repercusión de daño que este mal podría causar a nuestro país; en la presente tesis, se plantea un enfoque sobre esta nueva forma de hacer terrorismo, resaltando la importancia que el tema posee y haciendo un análisis descriptivo del caso; que se espera sirva de instrumento para la elaboración de normas legales que permitan mecanismos de control

en base a seguridad informática. Así mismo, se plantea el mejoramiento de sistemas informáticos, pero no solamente en los elementos software y hardware, sino primordialmente en el elemento humano, que deberá ser capacitado con ayuda de organismos internacionales que ya manejan el tema y ofrecen apoyo en la lucha contra el Ciberterrorismo.

Por lo mencionado anteriormente, este tipo de ataque no utiliza arsenales para cumplir objetivos de destrucción, mas por el contrario, emplea medios informáticos.

Los medios informáticos como la computadora y redes, son manipulados ahora, por un gran número de personas en todo el mundo. Pero pocos son los que utilizan esta tecnología para provocar daño, o intimidar a otras personas.

De tal manera, es que se establece que quién ataca y rompe medios de seguridad para introducirse en sistemas informáticos con el fin de causar destrucción y muerte utilizando el miedo, es el **terrorista informático**; persona altamente calificada en programación y desarrollo de sistemas informáticos. Pero además, capacitado en técnicas terroristas que implican destrucción masiva de objetivos; ya que al atacar sistemas informáticos, se debe conocer el punto estratégico que emplea muchas variables, para colapsar todo un sistema.

1. PLANTEAMIENTO DEL PROBLEMA

El problema se origina, a través de la aparición de nuevos medios informáticos utilizados por los terroristas, a fin de atemorizar, destruir, causar zozobra y desestabilizar el orden constitucional de un determinado Estado; con el riesgo de penetrar en sistemas informáticos de uso ciudadano, militares, policiales, e inclusive de seguridad nacional de todos los países incluido el nuestro.

Identificable por la destrucción que se realiza de forma virtual a través del uso la red de redes (Internet); empleando de tal forma medios informáticos, donde no es necesaria la presencia física del terrorista. Situación que hace más complejo el tema ya que la autoría y ubicación del delincuente se hace más complicada, debiendo por lo tanto desarrollarse un estudio sobre el terrorismo

informático. Además de la consiguiente perspectiva jurídica que configura su accionar.

1.1. PROBLEMATIZACIÓN

Los Ordenadores controlan de forma automática muchos procesos: control de aguas, reparto del fluido eléctrico, conmutación de una central telefónica, control de tráfico aéreo, etc. Situación que es aprovechada por los ciberterroristas, quienes ingresando a los sistemas informáticos que controlan equipos electrónicos de los cuales depende el funcionamiento de los servicios mencionados; logran colapsarlos y provocar daños materiales, e inclusive la muerte de muchas personas.

Por lo que el Ciberterrorismo se convierte en un problema al atentar contra la Soberanía del Estado; causar pánico, zozobra e inclusive la muerte de personas; así como la destrucción de infraestructuras a través de medios informáticos. Más aún conociendo que el acceso a los sistemas informáticos de control sobre servicios críticos que utiliza el gobierno y las empresas privadas carecen de una seguridad eficiente.

Por todo ello es que el Terrorismo Informático, alcanza parámetros que deben ser contemplados jurídicamente, partiendo de la perspectiva integral que posee.

De tal forma, convendría plantearse, las siguientes interrogantes: ¿Existe la una adecuada conciencia del problema en nuestro país?; ¿Existen medios de protección

ante ataques ciberterroristas?; si los hay, ¿Son adecuados?; ¿Nuestro derecho positivo, considera los medios utilizados por el terrorista informático?; ¿Cuál el alcance real de daño con el uso de medios informáticos con fines terroristas?; ¿El Terrorismo Informático, merecerá una adecuación normativa de alcance integral?.

2. DELIMITACIÓN

2.1. TEMÁTICA

CUANDO

La presente Tesis, se introduce en el tema, delimitando en su contexto la figura del terrorismo informático desde un estudio que comprende sus características, clasificación, medios y lucha para combatirlo; estableciendo principalmente que el accionar del ataque ciberterrorista puede producirse en cualquier momento y de forma secuencial; es decir, que no existe una hora, ni fecha determinada, pero sí podría existir una cadena de ataques originados en distintos sitios geográficos, enfocándose a mismo objetivo, y en reiteradas oportunidades por lapsos de tiempo calculados de acuerdo al daño que se quiera causar.

DONDE

Si bien el ataque se produce en el ciberespacio, posee un punto físico de origen, donde el terrorista utilizando medios informáticos (la computadora) e introducido en una

red de control del sistema informático al que se quiere atacar; empieza su misión en deterioro del objetivo.

El ataque podría originarse desde diferentes sitios geográficos, utilizando el ciberespacio como canal de ejecución de objetivo. Sin embargo, la difícil localización del ataque terrorista, hace que no se pueda establecer con precisión las coordenadas de origen, ni tampoco la futura actuación terrorista, por lo que el control solo se puede establecer en base a direcciones IPS de computadora, que no son cien por ciento seguras, pero ayudan a su localización.

QUE

Tomando en cuenta el alcance mundial que el terrorismo informático ha logrado dentro de los últimos años, y la repercusión de daño que este mal podría causar a nuestro país; en la presente Tesis, se resalta la importancia jurídica que el tema posee y se hace un análisis descriptivo del caso; a fin de constituirse en un instrumento de estudio para la elaboración de normas legales integrales que permitan la creación de mecanismos de control en base a seguridad informática. Así mismo, se plantea el mejoramiento de sistemas informáticos, pero no solamente en los elementos software y hardware, sino primordialmente en el elemento humano, que deberá ser capacitado con ayuda de organismos internacionales que ya manejan el tema y ofrecen apoyo en la lucha contra el Ciberterrorismo.

QUIEN

Los medios informáticos como la computadora y redes, son manipulados ahora por un gran número de personas en todo el mundo con diferentes fines; sin embargo, existen grupos terroristas que utilizan esta tecnología para lograr sus objetivos.

El **terrorista informático**; persona altamente calificada en programación y desarrollo de sistemas informáticos y capacitado en técnicas terroristas que implican destrucción masiva de objetivos, es considerado el sujeto de investigación en el presente trabajo.

POR QUE

El terrorista hoy en día, no solo utiliza los medios llamados tradicionales en su accionar; sino también emplea medios que la tecnología pone a disposición, tales como los informáticos.

De tal forma, que este tipo de terrorismo se ha constituido en el medio de ataque tal vez más eficaz, por las diferentes ventajas que lo diferencian de las demás otras formas de terrorismo, como el terrorismo por alcance, por blancos, histórico, global, etc.

2.2. TEMPORAL

El presente trabajo se circunscribe al descubrimiento del Terrorismo Informático, realizado por Andy Marshal en el año 1976, y su repercusión hasta el 2.004.

2.3. ESPACIAL

Se delimita espacialmente en función al ciberespacio, sus plataformas virtuales y el contexto jurídico boliviano.

3. JUSTIFICACIÓN

El desarrollo tecnológico que día a día experimentamos, hace que surjan nuevas formas de delincuencia que deben ser controladas por políticas preventivas adecuadas y disposiciones legales eficaces en todos los países a nivel mundial.

Algo que sin duda esta desarrollándose de manera precipitada y casi incontenible, es el tema del terrorismo. Países como Estados Unidos y otros tecnológicamente desarrollados, no han podido contrarrestarlo de forma definitiva, pese al gran presupuesto que han introducido para combatirlo.

De tal forma el Terrorismo ensancha su nivel operativo y encuentra nuevas formas para lograr su objetivo causando terror, pánico y zozobra, debilitando de tal manera el orden constitucional de los Estados; e incorporando en su accionar el uso de instrumentos informáticos, generándose así el Ciberterrorismo.

La importancia del tema adquiere una profunda relevancia jurídica y social; ya que se funda en la falta de información que existe sobre el terrorismo informático en la población y la consiguiente desprotección jurídica al respecto; sin embargo, la sanción de una ley integral adecuada, no podrá realizarse, si antes no se funda suficientemente el problema.

La perspectiva jurídica que genera el Terrorismo Informático, conlleva no solo la modificación de nuestra normativa penal sustantiva en cuanto a la sanción del hecho; sino conlleva un tratamiento jurídico integral, ya que deben enfocarse medidas de seguridad, concientización y control adecuado.

4. OBJETIVOS

4.1. OBJETIVOS GENERALES

Enfocar la perspectiva jurídica que el Terrorismo Informático conlleva, a fin de resguardar la Soberanía del Estado; proteger la seguridad y el orden constitucional del mismo así como resguardar la vida e integridad de las personas junto con la infraestructura pública y privada ante caberataques.

Lograr la concientización del Estado y la población en general, sobre el peligro que involucra la utilización de medios informáticos ante su empleo por terroristas.

4.1. OBJETIVOS ESPECÍFICOS

Identificar los medios, recursos y tácticas que emplea el terrorista informático, así como su perfil, blancos preferidos y estrategias utilizadas.

Realizar un estudio comparativo de la normativa legal vigente de todos los países en materia de terrorismo informático.

Efectuar un análisis de las acciones de represión que realizan Instituciones y Organismos Internacionales para combatir al terrorismo informático.

Identificar los vacíos legales que nuestra legislación posee con respecto a la lucha y sanción del Terrorismo Informático.

Evidenciar la necesidad que tiene nuestro país, de suscribir Convenios y Acuerdos Internacionales que combatan y castiguen al Terrorismo Informático, otorgando de tal forma al Estado un apoyo internacional sobre el tema. Debido a la mala implementación en seguridad informática que posee.

5. HIPÓTESIS

A través del análisis del Terrorismo Informático y su consiguiente perspectiva jurídica se logrará resguardar la Soberanía y el orden constitucional del Estado; resguardar la vida e integridad de la población así como la infraestructura pública y privada ante ataques Ciberterroristas; concientizando al Estado y a la población en su conjunto sobre el peligro que representa que el terrorista utilice medios informáticos para causar pánico y zozobra; involucrando para ello una posterior adecuación de la norma positiva de nuestro país.

6. VARIABLES

6.1. INDEPENDIENTE

El desconocimiento sobre los medios informáticos que utiliza el terrorista para el deterioro de la estabilidad constitucional de un Estado.

6.2. DEPENDIENTES

Provoca la inadecuada protección a los sistemas informáticos existentes.

Configura un vacío legal del que nuestra norma positiva adolece en cuanto a la tipificación del delito de terrorismo en el Código Penal y la inexistencia de una ley especial

Vulnera los derechos reconocidos por nuestra Constitución Política del Estado.

Atenta contra la Soberanía de nuestro país.

7. METODOLOGÍA

La ciencia dispone de una variedad de métodos para el conocimiento, debido a que la realidad material del mundo en que vivimos, es por su naturaleza totalmente diversa, y cada uno de sus procesos y problemáticas exigen un enfoque especial para su investigación. Por ello es que en función al Método científico y la variada existencia de métodos, el presente Trabajo, rescata para

su desarrollo al Método Jurídico, Dogmático y al Deductivo, así como técnicas que permiten su aplicación.

La Metodología empleada en el presente trabajo, es de carácter descriptiva, explicativa y propositiva; ya que mediante la descripción de los medios informáticos utilizados por el terrorista informático, se explica la aparición de la figura del Terrorismo Informático, así como la eficacia en su accionar y su consiguiente perspectiva jurídica.

El Método Jurídico, enfoca una problemática tridimensional del Derecho. Es decir que existe una realidad histórica - cultural, un hecho emergente y la existencia de un valor que determina el hecho.

Al mencionar a la realidad histórica – cultural, se establece que durante el transcurso del tiempo en el que el Terrorista, ha buscado la concreción de sus ataques a fin de crear miedo y zozobra en la población; ha adoptado el uso de nuevos medios para la concreción de sus crímenes, encontrando de tal forma a los medios informáticos, como instrumentos eficaces.

Un tema muy importante, es el hecho de que nuestra cultura, se resiste de alguna manera ante el avance tecnológico; menospreciando la adecuación que los terroristas pueden dar a los medios informáticos y afirmando que los ataques no podrían realizarse en nuestro país, ya que el mismo no se halla a la altura tecnológica de otros.

Sin embargo, la realidad es que en nuestro país, existe la tecnología adecuada; ya que bastará con una Terminal (computadora), conectada a Internet y su consiguiente empleo en ataques a sistemas críticos de control sobre servicios básicos.

Esta realidad mencionada, involucra la desatención en la perspectiva jurídica que la figura del Terrorismo Informático presenta; existiendo desconocimiento en la población al respecto.

El valor asignado a este hecho emergente, se constituye en el respeto a nuestra soberanía y la adecuada concientización que se debe dar ante el daño que puede ocasionar las acciones del Terrorismo Informático.

El Método Dogmático, también utilizado en el presente Trabajo, recibe también el nombre de Método Teórico, el cuál tiene como finalidad la evaluación de las estructuras del derecho, concibiendo el problema jurídico desde una "…perspectiva estrictamente formalista…" **([1])**. Es decir que se emplea un análisis del derecho en función a la norma tal cuál establece su articulado, lo que permite descubrir los vacíos jurídicos existentes.

La presente Tesis, enmarca su investigación dentro de un método que respeta el Derecho positivo de nuestro país, se encuadra en él y fundamenta la necesidad de análisis de la perspectiva jurídica que conlleva el Terrorismo Informático.

Otro método empleado es el Método Deductivo, conceptuado como aquel que parte de datos generales aceptados

[1] WITKER, Jorge, "La Investigación Jurídica", pág. 59

como válidos, tal es el caso la utilización de medios informáticos por terroristas a nivel mundial y la contemplación normativa que debe tener, y que a través de un razonamiento lógico deriva en el hecho de que Bolivia no se encuentra ajena y vulnerable ante ataques ciberterroristas; puesto que posee las mismas cualidades de la mayoría de los países.

8. TÉCNICAS

La técnica empleada para el desarrollo de la Investigación, fue la recopilación de datos bibliográficos, a través de libros, Internet y de elaboración propia.

CAPITULO I

EL TERRORISMO

1.1. ANTECEDENTES DEL TERRORISMO

Al realizar una revisión cronológica del terrorismo; nos encontramos con el hecho de que desde tiempos muy antiguos y hasta nuestros días, la comisión de este delito, ha ocasionado graves consecuencias.

El terrorismo considerado un delito polimorfo por Ribo Durán.([2]), debido a que puede revestir formas muy distintas de delitos; ha experimentado con el pasar del tiempo, cambios en su manifestación, utilización de medios y repercusión; de tal manera es que se ha dividido a la historia del terrorismo en la presente tesis en: Las Culturas Primitivas; Grecia y Roma; El Despotismo Ilustrado con sus luchas libertarias del siglo XVIII; El Terrorismo Contemporáneo del siglo XIX y principios del XX y el Neo Terrorismo, donde la aparición de armamento químico, medios informáticos y dominio sobre la información crean un peligro latente para toda la humanidad.

1.1.1. CULTURAS PRIMITIVAS

Dentro de las culturas primitivas, encontramos al típico brujo de la tribu, quién acudía al terrorismo físico y

[2] RIBO, Luís, "Diccionario de Derecho", Pág. 608.

"mágico", para imponer su autoridad y poder sobre los demás miembros.

Esta antigua forma de terrorismo, no tenía una unidad ideológica clara. Ya que los atentados terroristas, podrían haber sido motivados por lealtades divinas, complots y generalmente solo para asesinar a un opresor. Inclusive, en este tipo de acciones, se calificaba al asesino de "héroe", ya que se encontraba legitimidad en su accionar al castigar con la muerte a un jefe tribal déspota.

1.1.2. GRECIA Y ROMA

Más tarde, durante el Imperio Romano existieron diversos casos de Terrorismo de Estado, entre los que se incluyen la supresión brutal de los seguidores de Espartáco después de la Rebelión de los Esclavos del 73-71 d.C., así como la eliminación y la esclavización de la nación Dacia en 106 d.C. Asimismo, en los territorios conquistados los romanos imponían su autoridad sin tener compasión.

El levantamiento de los griegos de Jonia contra Darío hacia el 499 AC. fue el desencadenante de una de las más famosas cadenas de acciones Terroristas de la antigüedad: las erróneamente conocidas como "Guerras Médicas" en las que grupos armados de toda la Hélade enfrentaron al imperio persa en su intento de exportar el orden a occidente.

Pero posiblemente corresponda a Roma (República e Imperio), el trágico honor de haber soportado la mayor cantidad de atentados, acosos, revueltas y acciones terroristas por todo lo largo y ancho de su infinito territorio.

Ya en el 298 AC, una coalición de violentos formada por samnitas, etruscos, celtas, sabinos, lucanos y umbros tuvo que ser ejemplarmente aplastada por las legiones imperiales con objeto de ir ensanchando las fronteras de la ley y de la paz (*la pax romana*).

Después aparecerían: Vercingetorix en la Galia o Viriato en Hispania que asediaron con saña a las tropas civilizadoras romanas mientras transformaban dos paraísos naturales en útiles graneros y almacenes, acabando con las prácticas salvajes y domesticando territorios y personas. La resistencia irracional y fanática demostrada por los violentos en Numancia, Astapa o Calagurris retrata perfectamente el carácter cerril y montaraz de estos grupos armados que no dudaron en utilizar a la población civil como escudos humanos provocando así su aniquilación.

Ya después de Cristo, el Imperio hubo de enfrentarse a terroristas númidas y beréberes donatistas, y a violentos separatistas cántabros y vascones, especialmente a los temibles grupos armados conocidos como Bagaudas, durante los siglos III y IV.

1.1.3. DESPOTISMO ILUSTRADO (SIGLO XVIII)

En este periodo, se puede encontrar a un sin fin de reyes y emperadores, que si bien protegían las ciencias y las artes; también ejercían gobiernos despóticos que se basaban en el terrorismo. Dentro de este Despotismo Ilustrado, al mismo tiempo, se desarrollaban ideas liberales y revolucionarias que dieron origen a la Independencia de los Estados Unidos en 1776; a la Revolución Francesa de 1789 y a la Guerra Civil Hispano-Americana, donde nació la independencia de las naciones Americanas a partir de 1808.

Para los gobernantes de este periodo, el terrorismo se había convertido en un medio de defensa contra las tendencias liberales

1.1.4. TERRORISMO CONTEMPORANEO (SIGLO XIX)

Siglo donde se destaca la historia del terrorismo en Rusia, donde se practicaba este delito por ambos lados; es decir, que el gobierno Zarista realizaba actividades terroristas para mantenerse en el poder; y los conspiradores, también lo utilizaban para suprimir al zarismo, imponer una constitución y distribuir las tierras entre los campesinos.

Uno de los mayores representantes del Absolutismo y terrorismo europeo, fue Nicolás I, quién una vez que desbarató a la conspiración anti-zarista, declaró

públicamente que no tendría piedad ni ninguna misericordia con los jefes de ese movimiento conspirador.

Más adelante, Alejandro III quiso eliminar a los terroristas, pero estos se hacían cada vez más fuertes difundiendo las doctrinas marxistas.

Posteriormente, con el triunfo de Lenin, el terrorismo se convierte en una norma dentro de Rusia.

A finales del siglo XIX, el Terrorismo Anarquista, se difundió por toda Europa; realizando las actividades más violentas y sanguinarias del anarquismo revolucionario que buscaba destruir a la sociedad organizada. Perpetrando atentados con bombas sobre multitudes, generalmente en teatros y en otros lugares de concurrencia numerosa y desprevenida.

Las medidas de prevención contra el Terrorismo Anarquista, se desataron en todo el mundo. Generando que la policía de todos los países realice un control exhaustivo de todos los extranjeros que ingresaban a su territorio y cuya permanencia presentaba sospechas. Se tipificó al Terrorismo, como un delito gravísimo, sancionado en algunas regiones con la pena de muerte.

1.1.5 NEO TERRORISMO.

Sin lugar a dudas, después de haber experimentado una variedad de tipos de terrorismo durante el pasar del tiempo; en la actualidad, las medidas antiterroristas van

orientadas a controlar, cada vez más, tanto el Internet, como los contenidos que por él transcurren. Esta tendencia se explica por la manipulación tecnológica que se hace de la información y los medios químicos. Situación que será detallada en el Capitulo II de la presente Tesis, en lo referente a los nuevos medios utilizados en la actualidad por las agrupaciones terroristas.

1.2. CONCEPTO Y DEFINICION

La palabra terrorismo se desprende de terror, que proviene del latín "***terroris***" que significa miedo muy intenso.

Walter Laqueur entiende al terrorismo como "el empleo o amenaza de violencia, un método de combate o una estrategia para lograr ciertos objetivos, con el propósito de inducir un estado de temor en la víctima que no se ajusta a las normas humanitarias y en cuya estrategia es fundamental la publicidad" **([3])**

El Diccionario de la Real Academia de la Lengua, establece que terrorismo: "Es la dominación por el terror; y la sucesión de actos de violencia ejecutados para infundir terror".

La Enciclopedia Electrónica Encarta, conceptualiza al terrorismo como: "el uso de la violencia, o amenaza de recurrir a ella, con fines políticos, que se dirige contra víctimas

[3] BARTOLOMÉ, Mariano César, Citado en "El terrorismo como amenaza transnacional". Conferencia dictada en el Primer Seminario sobre Seguridad Pública, auspiciado por el Gobierno de la Provincia de Tucumán, noviembre de 1997. Ver texto completo en http://www.ba.ucsa.edu.ar/isco/doc/Tr4.htm

individuales o grupos más amplios y cuyo alcance trasciende con frecuencia los límites nacionales. El término implica una acción llevada a cabo por grupos no gubernamentales o por unidades secretas o irregulares, que operan fuera de los parámetros habituales de las guerras y a veces tienen como objetivo fomentar la revolución". **([4])**

Por su parte la Enciclopedia Jurídica Omeba, señala que Terrorismo es la "Doctrina política que funda en el terror sus procedimientos para alcanzar fines determinados. El terrorismo no es por lo tanto un fin sino un medio" **([5])**

Según el **Departamento de Estado de los Estados Unidos**, terrorismo, es "la violencia premeditada, perpetrada por motivaciones políticas contra objetivos no combatientes, por parte de grupos sub-nacionales o agentes clandestinos, usualmente con la intención de influir sobre el público" **([6])**

Cabanellas, por su parte señala que "son los actos de violencia y maldad ejecutados para amedrentar a ciertos sectores sociales o a una población determinada o para desorganizar una estructura económica, social y política". **([7])**

Por lo antes mencionado se puede definir al terrorismo como toda sucesión de actos para infundir terror, miedo,

[4] ENCARTA 2004, ENCICLOPEDIA ELECTRÓNICA. Microsoft Corporation.
[5] OMEBA, ENCICLOPEDIA ELECTRÓNICA JURÍDICA – TOMO XIX Derecho Penal, Sección Delitos Pág. 126.
[6] DEPARTAMENTO DE ESTADO DE EEUU.- http//usinfo.state.gov/espanol/
[7] CABANELLAS, GUILLERMO, Diccionario Enciclopédico de Derecho Usual, Tomo VIII,Pág. 55.

zozobra; utilizando diferentes medios con el fin de lograr el cambio radical en el orden constitucional de un Estado.

1.3. PERFIL DEL TERRORISTA

El terrorista, por lo general, empieza con sus primeros atentados entre los 22 a 25 años; es predominantemente de sexo masculino, ya que la membresía femenina constituye menos de un dieciséis por ciento y su labor normalmente consiste en servicios de salubridad y de atención doméstica al albergue terrorista.

El terrorista mayormente es soltero. Ya que las actividades que realizan, les impide preocuparse por algún tipo de responsabilidad familiar.

Son personas que con frecuencia son ignoradas dentro del proceso gubernamental y la toma de decisiones. Y como forma de rebelión usan la violencia para hacerse escuchar.

Personas hiperactivas, ya que la inactividad puede causar inquietud en las organizaciones terroristas.

Se debe tomar en cuenta, que los terroristas siempre se encuentran alertas y de alguna manera un paso delante de nosotros.

1.4. TIPOS DE TERRORISTAS

1.4.1. TERRORISTAS CLÁSICOS

Los terroristas típicos o clásicos, son aquellos que perpetran el acto terrorista y después intentan escapar, para lograr salvar su vida; con el propósito de continuar con su objetivo.

Este tipo de terroristas, en un noventa por ciento, no tienen familia en primer grado; dedicando su tiempo exclusivamente al fin u objetivo de la organización.

1.4.2. TERRORISTAS SUICIDAS

Estos terroristas, son del tipo Kamikaze; es decir que están dispuestos a morir en nombre de su causa. Este tipo, cumple al pie de la letra las órdenes emanadas por su organización; que por lo general se basa en la dominación religiosa, presión psicológica y la indoctrinación.

Los terroristas suicidas, se han separado totalmente de su familia, o esta es inexiste. Motivo por el cuál perpetran el delito en pro de su causa, sin importarles que para ello tengan que sacrificar su vida; ya que ésta es insignificante en relación a la lucha que realizan por el objetivo que profesan.

1.5. OBJETIVOS

Si bien los objetivos perseguidos por los terroristas son variados, se ha tratado de enumerar a algunos de ellos:

- publicidad para su causa;
- lograr el reconocimiento político;
- lograr bajas de civiles inocentes, para causar miedo en un Estado;
- ofender y mellar la dignidad humana;
- colapsar el sistema financiero;
- desarrollar la inseguridad en la población, logrando que la gente no pueda sentirse tranquila en ningún lugar;
- someter a la gente a su religión.

1.6. CARACTERISTICAS

- es una forma de lograr temor;
- incrementa el miedo;
- tiene una dinámica propia;
- busca su publicidad;
- en algunos países o regiones, el terrorismo se encuentra protegido por las autoridades del lugar;
- se constituye en el aglutinamiento de fuerzas y células homogéneas que se esconden;
- los grupos deben probar su credibilidad, generando la creencia de que ellos tienen más poder, mayor apoyo popular y más influencia que la real;
- las víctimas de las acciones terroristas, no son necesariamente el objetivo de los terroristas;

1.7. MEDIOS PARA COMBATIRLO

1.7.1. NO HOME

Se debe negar todo asilo y vivienda física al terrorista. Normalmente, los terroristas buscan refugio dentro de la población; sin embargo, más que tratar de identificarse con una lucha delincuencial perpetrada por estos sujetos, la comunidad debe entender de que no se puede combatir determinada situación, con la perpetración de un acto terrorista, ya que este se configura en un delito, que ocasiona inclusive la muerta de personas inocentes.

El brindar albergue a terroristas, involucra facilitar al delincuente la comisión del hecho delictivo. Lo que también se configura en un delito, que dentro de nuestra legislación se encuentra tipificado en el Artículo 23 del Código Penal; el cuál señala que son cómplices los que de cualquier otro modo facilitan o cooperan a la ejecución del hecho, en tal forma que aún sin esa ayuda se habría cometido y los que en virtud de promesas anteriores, prestan asistencia o ayuda con posterioridad al mismo. **([8])**

1.7.2. NO TRAINING

No se debe otorgar facilidades de entrenamiento al terrorista. Es decir, se debe realizar un control exhaustivo de las personas que

[8] Código Penal Boliviano, Parte General, Art. 23.

buscan asesoramiento o entrenamiento en determinadas acciones o actividades militares, policiales o de seguridad.

En el caso del atentado del 11 de Septiembre, se ha podido evidenciar que los perpetradores terroristas, recibieron dentro de los Estados Unidos, capacitación en el manejo de aeronaves, lo que les permitió adentrarse en las políticas de navegación aérea de este país e introducirse en una selección de pilotos en vuelos comerciales. **([9])**

1.7.3. NO FINANCE

El impedir cualquier tipo de financiamiento que se presuma vaya orientado al desarrollo de actividades terroristas, es el deber de toda la población.

Dentro de la variedad de formas que los terroristas utilizan para lograr financiamiento; se encuentra al narcotráfico y la captura de rehenes para obtener un posterior rescate. Motivos por los cuáles se debe destacar e incorporar como prioridad nacional, la lucha y prevención contra estos delitos.

1.7.4. NO MORAL GROUNDS

[9] http://www.fbi.gov/library/terror/95report/terrusa.html

No se debe dar, ningún tipo de ayuda moral y psicológica por parte de la población. Por lo general, el terrorista busca apoyo del pueblo, con el ardid de que defiende algún tipo de consigna popular.

Si bien es verdad que la población de casi todos los países, se encuentra impotente de poder resolver problemas como la corrupción, pobreza y abuso de autoridad, de ninguna manera debe identificarse con supuestos "defensores de la sociedad", que bajo la consigna de luchar contra el opresor cometen actos delincuenciales, que llegan inclusive a la muerte de civiles inocentes.

El hecho de dar apoyo moral a los terroristas, mediante la aceptación o sumisión de sus actos; de ninguna manera se constituye en legitimar las acciones terroristas; sino más bien se configura en complicidad, tipificada en nuestra normativa y señalada anteriormente.

1.7.5. OTROS MEDIOS

Se debe hacer hincapié, que la promoción de la democracia dentro de los regímenes dictatoriales y totalitarios; es una forma muy acertada de prevenir al terrorismo.

De todas formas, si se pretende erradicar al terrorismo del contexto mundial. Primeramente se

debe combatirlo y eliminarlo de nuestro país. Aún sabiendo que será una larga lucha; y tal vez encubierta por grupos de poder; muy costosa y de largo alcance; donde lamentablemente mueran muchas víctimas civiles inocentes. Pero esta es una guerra que debemos empezar lo más antes posible, empezando con la concientización del problema a la ciudadanía, para lograr formar un frente amplio que preserve nuestro planeta para nuestros mismos herederos.

1.8. ATAQUES TERRORISTAS A ESTADOS UNIDOS (11 DE SEPTIEMBRE)

El 11 de septiembre de 2001; se ha convertido en una fecha inolvidable para todo el mundo. Ese día, una manifestación realmente sorprendente de terrorismo cobro millares de vidas en los Estados Unidos de América. Vidas de personas inocentes fueron atacadas por sorpresa, cuando aviones comerciales se estrellaron contra las Torres Gemelas de New York (Símbolo del poder económico y del desarrollo tecnológico de EEUU) y el Pentágono, Sede Administrativa de las Fuerzas Armadas (expresión del mayor poder militar del mundo).

Los organismos de seguridad de Estados Unidos, aseguran que los responsables de los ataques del 11 de septiembre se sirvieron de Internet desde lugares públicos para comunicarse, evitando así ser detectados por las autoridades. Por su parte, la

Oficina Federal de Investigaciones (FBI) y la Agencia Central de Inteligencia (CIA) además de otras oficinas de seguridad alrededor del mundo, han reportado un aumento alarmante del uso del computador con conexión al Internet por parte de grupos terroristas. Los informes aun con anterioridad de los inesperados acontecimientos, indican el acceso no autorizado a bases de datos estatales donde se extrae información confidencial y se introdujeron virus con el objetivo de alterar los sistemas de comunicación de gobiernos, ejército y grandes corporaciones privadas o hacerlos inservibles. **([10])**

Lo ocurrido en los Estados Unidos desde el 11 de septiembre hasta la fecha nos lleva a pensar que la Internet retrocede en sus propósitos y se ubica de nuevo, por fuerza de las circunstancias o quizás por estrategia, en los objetivos iniciales para la que fue creada por sus padres fundadores **([11])**. Efectivamente, la red Internet fue pensada como una red para la guerra. Y esa idea lamentablemente continúa hasta hoy. Por ello, no debe extrañar que en este espacio virtual ocupado por la red, se vayan a crear nuevas generaciones que involucren la participación de nuevos actores (soldados informáticos).

1.8.1. ORDEN MILITAR SOBRE "DETENCIÓN, TRATO Y JUICIO DE CIERTOS NO-CIUDADANOS EN LA GUERRA CONTRA EL TERRORISMO".

[10] http://www.fbi.gov/library/terror/95report/terrusa.htm

[11] MATHIAS, Paul (1998). La ciudad de internet. Biblioteca del Ciudadano, pág. 11. "…El Internet nació como proyecto técnico para la guerra que, desde finales de la década del setenta, hizo concebir a los militares estadounidenses la esperanza de dotarse de un sistema informático indestructible. La deslocalización de los centros nerviosos de la ARPANET (Advanced Research Projects Agency Net: Red de la agencia para los proyectos de tecnología avanzada)".

A través del Public Law 107-40, 115 Stat. 224; y las secciones 821 y 836 del Título 10 del Código de los Estados Unidos de América; el Congreso de este país, otorga al Presidente George W. Busch, la "Autorización para el empleo de la Fuerza Militar".

Y a raíz de los ataques terroristas del 11 de septiembre, el Congreso de los Estados Unidos de América dotó a su presidente de amplios poderes para poder encarar los atentados perpetrados. Por ello, el 13 de noviembre de 2001, Busch dictó, en su envestidura de presidente y en su calidad de Comandante de las Fuerzas Armadas; una Orden Militar sobre "Detención, trato y juicio de ciertos no-ciudadanos en la guerra contra el terrorismo".

Dentro de de esta Autorización, en la Orden Findings (la motivación del instrumento legal); se señala la exposición de motivos para esta determinación; contemplando:

a) terroristas internacionales incluidos los miembros de Al Qaeda, crean un estado de conflicto armado;
b) se establece la Declaración de Emergencia Nacional con motivo de los ataques terroristas a través del Proc. 7463;
c) los terroristas poseen tanto la capacidad como la intención de llevar adelante nuevos ataques de este género;
d) la posibilidad de prevenir esos ataques, proteger a los Estados Unidos y a sus ciudadanos y apoyar esfuerzos similares por parte de países aliados, depende en forma significativa del empleo de las Fuerzas Armadas

Norteamericanas para identificar a los terroristas y a quienes les brindan colaboración, impedir sus actividades y eliminar su capacidad de conducir o sustentar estos ataques;

e) es necesario que los responsables de tales conductas criminales sean juzgados por violaciones a las leyes de la guerra y otras leyes aplicables, por tribunales militares;
f) no es posible aplicar en las comisiones militares los principios de derecho y las reglas de prueba generalmente reconocidos en el enjuiciamiento penal por parte de las Cortes Distritales de los Estados Unidos; y
g) la magnitud de los hechos que es necesario enfrentar implica que existe una emergencia extraordinaria para efectos de defensa nacional, que esa emergencia implica un urgente y apremiante interés del gobierno, y que es necesaria la expedición de la presente Orden para hacer frente a la emergencia.

Algo que llama la atención, es que solamente es aplicable a extranjeros y no así para estadounidenses.

En otra parte de la Orden, aparecen disposiciones esenciales de carácter penal sustantivo. Donde se establece su ámbito de aplicación (EEUU); una descripción de las conductas punibles; los procedimientos y las medidas a ejecutarse en torno al tema. Además, para que ser sometido a esta Orden, se requiere un acto de individualización presidencial, que establece que:

a) es o fue miembro de la organización denominada Al Qaeda;
b) ha participado en actos de terrorismo internacional o conspirado para cometerlos o prepararlos; que hayan

causado, puedan causar o se pretenda que causen daños o efectos adversos para los Estados Unidos de América, sus ciudadanos, la seguridad nacional, la política exterior o la economía;

c) ha brindado auxilio o encubierto conscientemente a aquél.

En lo referente a la detención; esta Orden, faculta al Secretario de la Defensa en Materia de Detención, quién debe precautelar la misma en lugares adecuados, fuera o dentro de los Estados Unidos; la provisión de alimento, agua, ropa y tratamiento médico adecuado; e incluso libertad para la práctica religiosa.

Otra sección rescatable, establece que:

a) el juicio de los inculpados se seguirá ante tribunales militares;
b) estos órganos podrán interponer las sanciones previstas por las leyes aplicables inclusive prisión perpetua o pena capital;
c) el Secretario de la Defensa dispondrá lo conducente para la constitución de las comisiones militares y el proceso mismo;
d) las disposiciones respectivas abarcarán, entre otros puntos, las etapas anteriores al juicio. Los procedimientos de juicio y las diligencias posteriores a éste, las pruebas el desarrollo del proceso y las cualidades que deben reunir los abogados participantes.

Como se puede apreciar en el resumen que se hace de la Orden mencionada y haciendo un análisis jurídico de la misma;

se puede establecer que la justicia militar desplaza a la civil, y se enmarca dentro de la dirección de un jefe militar, al que se halla sujeto el todo el sistema procesal.

En cuanto a los sometidos a esta Orden, la misma establece que:

a) la jurisdicción para conocer de los delitos previstos en la Orden corresponde exclusivamente a los tribunales militares; y
b) los inculpados no podrán someterse ni beneficiarse de procedimientos o recursos, directa o indirectamente, en otros tribunales de los Estados Unidos o de un Estado de estos, ni en Cortes de otras naciones o en tribunales internacionales.

Por todo lo señalado anteriormente; se puede afirmar que Estados Unidos de América ha desarrollado con la presente Orden Militar sobre "Detención, Trato Y Juicio de ciertos no-ciudadanos en La Guerra contra el Terrorismo", un verdadero régimen de excepción dentro de su justicia penal ya que la desplaza y la cambia por la justicia militar.

Ahora bien, haciendo un análisis, surge la controversia en cuanto a su legalidad. Ya que la presente Orden no es una ley; sino es un mandamiento del Ejecutivo (equivalente a un Decreto Supremo en la legislación boliviana). Que dentro de la pirámide de Kelsen, no puede establecerse como norma de derecho por encima de la Constitución Política de cada País; dentro del contexto legal que establece que toda persona goza de

derechos, deberes y garantías; a un juicio justo, a la libre defensa; a no ser juzgado por comisiones especiales sino por ante el órgano jurisdiccional competente en cuanto a materia; por un juez imparcial, independiente y competente.

Este desequilibrio sustantivo y procesal, otorgando facultades al Mando Militar, sobrepasando las atribuciones del poder judicial. En una clara muestra de desconocimiento total de las normas y ni que decir de los derechos humanos, es defendida por John Ashcroft, procurador estadounidense que señala que los terroristas "no merecen la protección de la Constitución de los Estados Unidos" ya que existen valores constitucionales para algunas personas (que son la mayoría), que se niegan a otros **([12])**

1.9. TERRORISMO EN SUDAMERICA

Los antecedentes de terrorismo en Sudamérica, enfocan un terrorismo primitivo, con características sanguinarias dentro de los pueblos indígenas; ya que en los pueblos dominaba la ley del más fuerte, y predominaba la voluntad de los caciques y brujos, que utilizaban el terror como forma de sometimiento.

Por otro lado, se debe mencionar la presencia de la Inquisición en América, la cuál actuó principalmente en México y Perú. Esta institución, utilizó el terror, como instrumento para el adoctrinamiento de la religión católica; donde se llego inclusive a la pena de muerte.

[12] JOSJ, Tryangiel, hace mención a John Ashcroft en su artículo "And Justice for…", 26 de Noviembre de 2001.

Dentro de lo que significó la Guerra Civil o la Revolución libertaria en Sudamérica, se produjo la lucha entre Consejistas españoles y Juntistas americanos; lo que produjo una división en los pueblos americanos. Situación que Simón Bolívar llamó "la guerra de muerte", que no era más que el inicio del terrorismo desencadenado por ambas partes, que condujo a la muerte de miles de personas.

Sin embargo, debe realizarse una clara diferenciación entre lo que significa revolución y terrorismo.

Entendiendo a la revolución como al cambio general, realizado por la fuerza y a menudo con violencia, que experimenta un orden social o político, llevado a cabo por un segmento considerable de la población de un Estado. La revolución es la solución política más extrema que puede adoptar un grupo de disensión, y tiene lugar cuando fallan los intentos legales y más moderados de lograr el reconocimiento o la reforma o cuando la ideología del grupo revolucionario aboga directamente por la modificación radical de la situación existente.

Las sociedades modernas se deben mucho a levantamientos pasados contra gobiernos represivos, condiciones económicas restrictivas o estancadas, y rígidas divisiones de clases. Por otra parte, las revoluciones han sustituido con frecuencia un mal por otro, al instrumentar medidas de dureza extrema, exaltar un liderazgo egocéntrico o afirmarse sobre la represión del pueblo. En ocasiones, excesos de esta naturaleza desencadenaron el triunfo de

contrarrevoluciones, estimuladas por los enemigos del cambio político. Un desafío repentino orientado contra un orden social establecido puede contribuir a que en la sociedad se produzca una respuesta que se signifique en un sentido opuesto por completo al buscado por los partidarios de la revolución.

Una revolución no es lo mismo que un golpe de Estado, que supone la toma repentina del poder estatal por parte de una pequeña facción o un miembro del gobierno y no tiene por qué causar un cambio amplio y profundo del sistema social. Habría también que distinguir entre revolución y revuelta o rebelión, que puede ser un intento revolucionario fallido, una expresión violenta de protestas que aspira a lograr un objetivo prefijado o tan sólo un cambio en el panorama político. El término revolución se aplica de forma más general a cualquier transformación histórica importante. Y no debe confundirse con terrorismo, ya que este último, busca crear zozobra y miedo en la población para crear un desequilibrio en un gobierno legal y legítimo, cuál no es el caso de la revolución.

Es evidente que al hablar de Sudamérica, identificamos diferentes agrupaciones terroristas; con objetivos y razonamientos diferentes. Sin embargo, en la mayoría de los casos se les ha llamado guerrillas, desestimando el sentido real de los fines que estas agrupaciones buscaban, junto con los medios que empleaban para su cometido.

Tomando el caso de Argentina, se puede mencionar a los Montoneros; organización revolucionaria que luchó contra el gobierno y oligarquía. Su ideología es una mezcla del Peronismo

y el Marxismo-Leninismo; cuyo objetivo es reunificar al movimiento peronista fragmentado y la oposición a los militares.

Por otra parte, cabe mencionar la presencia durante los 60's a los 70's, del Ejército Revolucionario Popular (ERP), que representaba a un grupo Trotskista. Organización que desapareció al morir su líder en 1976.

En Colombia, la presencia de las Fuerzas Armadas Revolucionarias Colombianas (FARC), representa al grupo terrorista más poderoso. Mismas que, con tendencia Marxista-Leninista, presenta vínculos con el narcotráfico, para poder sostener sus operaciones y la obtención de armamento.

Una combinación de ideologías de Castro, Guevara, Mao y Trotsky; se presenta con la organización terrorista M-19 o Movimiento 19 de Abril. Organización que está totalmente en contra de los Estados Unidos. Este grupo terrorista colombiano, inicio sus atentados con el robo de la espada de Simón Bolívar; posteriormente con la toma de la Embajada de la República Dominicana en su país.

En Perú, Sendero Luminoso es una organización terrorista también con tendencia Marxista-Leninista, que enfoca su accionar en contra del gobierno y los Estados Unidos. Sin embargo esta agrupación, se diferencia de las guerrillas peruanas de los 60's porque no resaltan al Che Guevara o a Fidel Castro como líderes; sino identifican a los indios originarios del Perú como los representantes de su consigna revolucionaria. Pero también se encuentra en este país, grupos como el

Movimiento Revolucionario Tupac Amaru, que de igual forma cometió agresiones en contra de la población civil; sembrando zozobra en ese territorio.

En Chile el Movimiento de Izquierda Revolucionario (MIR), fue fundado en 1995 por trotskistas; realizando actos terroristas entre 1969 y 1970. Sin embargo, fue en el gobierno de Allende que resaltó su presencia con la promoción de reformas agrarias. Después del golpe de 1973, los miristas, tuvieron que salir del país, y en la actualidad, se encuentran diseminados por Chile y países vecinos a este.

En Bolivia, se ha desarrollado una extensión del ELN Colombiano, denominado ELN-B (Ejército Nacional de Liberación de Bolivia), mismo que pretende ser el heredero de las actividades que en algún momento liderara el "Che" Guevara, en el territorio de Bolivia. Se supone que estaría dividido en pequeñas unidades y conformado, predominantemente, por algunos elementos de la población indígena. Últimamente, su nivel de actividad parece haber disminuido significativamente.

Además en nuestro país, se destaca la presencia del antiguo Ejército Guerrillero Túpac Katari (EGTK). Mismo que ha sido la principal insurgencia guerrillera que ha conocido Bolivia desde la del Ché Guevara en 1967 a 1968 ya que desde 1990 se pensaba que, debido a su inserción en las comunidades campesinas, podría convertirse en una versión aymara de fuerzas que en el Perú irrumpieron con el senderismo. **([13])**

[13] http://www.aymara.org/lista/archivo2002/msg00157.html

El EGTK no ha buscado incorporarse a los gobiernos, como ha sido el caso del M-19 colombiano; ni mantiene un discurso revolucionario radical como el entonces jefe senderista Abimael Guzmán; sino llama a destruir a la República boliviana y a que las comunidades andinas no reconozcan a ésta, a la par que deben conformar un Estado paralelo con sus respectivas fuerzas armadas, autoridades y símbolos. Uno de sus representantes fue Felipe Quispe "El Mallku".

Originariamente el EGTK provenía de las Ofensivas Rojas, un grupo clandestino que se proclamaba como marxista y leninista ortodoxo surgido en 1980. Esta organización producía varias veces al mes folletos donde acusaba al resto de la izquierda de renegar de Lenin pues buscaban insertarse en el entonces gobierno de la Unidad Democrática Popular (1982-1985), además que en algún momento llegaron a tener un discurso fuertemente obrerista y a dirigir o influir varios sindicatos mineros contando con presencia significativa desde Milluni hasta el norte de Potosí.

El Ejercito Túpac Katari opera principalmente en la zona del altiplano y en la frontera con el Perú (Chapare). Recluta a sus elementos, preferentemente, entre la población indígena. Sus ataques se dirigen contra objetivos tales como oleoductos, oficinas gubernamentales, torres de transmisión eléctrica y a veces también contra las iglesias mormonas. **([14])**

[14] www.ladecadadel70.com.ar/temasdedifusion/c87.htm

De alguna forma, y como consuelo, tal vez deberíamos pensar que Sudamérica, se encuentra alejada geográficamente de los terribles e innumerables conflictos bélicos que se desencadenan en actos terroristas. Pero esta situación no garantiza de ninguna manera la inmunidad, ya que nuestro continente, se encuentra inmerso dentro de la globalización y por ende acarrea consigo todos los problemas inmersos a esta realidad, como los adelantos tecnológicos que utilizan los terroristas para perpetrar sus actos.

CAPITULO II

CLASIFICACION DEL TERRORISMO

2.1. DE ACUERDO AL OBJETIVO

2.1.1. SEGÚN EL ALCANCE DEL OBJETIVO

2.1.1.1. TERRORISMO GLOBAL

"La novedad es que las organizaciones terroristas de alcance global aspiran a socavar, por todos los medios a su alcance, incluso los más violentos, los pilares de la legitimación política de ciertos Estados" **([15])**. Es por eso que se puede esperar que no solo serán las grandes potencias las que aspiren a lograr el poder absoluto; sino también, nuevos grupos con fines de destrucción.

Las potencias mundiales, han descubierto que el poder no es un bien eterno. El caso de la Unión Soviética dentro de lo que significó la guerra fría, es un claro ejemplo de ello. Pero, si bien existen países que compiten por el Poder de Estado sobre sus pares. Existen por otro lado, aquellos entes políticos que tratan de controlar los excesos de poder.

[15] SEPULVEDA, Bernardo, El Eje del Mal y su Destino Manifiesto, Pág. 2.

Uno de ellos es el Consejo de Seguridad de la Organización de las Naciones Unidas; quién establece de alguna manera las reglas que los diferentes Estados deben seguir para esta "lucha de poder"; logrando de tal manera legitimidad en el accionar de estos pueblos.

Dentro de los grupos terroristas que emplean este tipo de terrorismo se puede mencionar a:

2.1.1.1.1. AL QAIDA.

Fue creado por Osama Bin Laden a finales de 1980 para unir a los árabes que lucharon en Afganistán contra la unión soviética. Son ayudados en financiamiento, reclutamiento, transporte y entrenamiento por los islámicos Sunni (musulmanes ortodoxos opuestos a los Shiitas), extremistas de la resistencia de Afganistán. Trabaja para derrocar a los regímenes que considera "no islámicos". Pretende expulsar de los países musulmanes a los ciudadanos occidentales y no afines a su religión.

Emite declaraciones bajo la bandera del Frente Islámico

Mundial por la Guerra Santa contra el deber de todo musulmán de matar a los ciudadanos estadounidenses (civiles o militares) y sus aliados, dondequiera que estén. Adjudicándoseles el atentado terrorista perpetrado el 11 de Septiembre a las Torres Gemelas en EE.UU.

2.1.1.1.2. BAADER-MEINHOF

El 2 de abril de 1968 cuatro jóvenes alemanes ingresan a los supermercados Schneider de Frankfort y siembran en sus tres pisos una docena de bombas incendiarias que minutos más tarde destruirán gran parte de la construcción. El atentado era una forma de protesta en contra de la "masacre" norteamericana en Vietnam.

Habiendo parado su accionar terrorista por un tiempo, reaparecerán el 27 de julio de 1976 secuestrando un avión de Air France que volaba de París a Tel Aviv con 240 pasajeros a bordo,

gran parte de ellos de origen judío. Desvían la nave hacia Entebbe, Uganda, tras lograr que el dictador Idi Amín autorizara su aterrizaje.

2.1.1.2. TERRORISMO FOCAL

Este tipo de terrorismo, concentra sus ataques en determinados objetivos; es decir se focaliza o concentra solamente en la destrucción por ejemplo de determinada étnia, grupo religioso, políticos de derecha, etc.

No toma en cuenta la dimensión geográfica de la ubicación de esta focalización; pudiendo perpetrar atentados en diferentes países o regiones.

Algunos de los grupos terroristas que ejecutan el terrorismo focal son:

2.1.1.2.1. HAMAS

Grupo palestino que persigue la creación de un Estado islámico palestino que reemplace a Israel.

Hamas surgió el 14 de diciembre de 1987, formado por el jeque Ahmed Yassim. Se derivó de

la rama Palestina de la Hermandad Musulmana, fundada en Egipto, que operaba en la Franja de Gaza, Judea y Samaria.

Es un movimiento social, religioso y político con una ideología radical que tiene dos objetivos centrales: terminar con los acuerdos de paz, y a través de la Jihad (la guerra santa) lograr la creación de un Estado islámico en todo el territorio de la antigua Palestina.

2.1.1.2.2. HÉZBOLA.

También conocido como Jihad Islámica, Organización de Justicia Revolucionaria de los Oprimidos de la Tierra, y la Jihad Islámica para la Liberación de Palestina.

Es un grupo radical shiita pro-iraní fundado en el Líbano en 1982. Pretende el establecimiento de una república islámica semejante a la iraní en el Líbano y la eliminación de toda influencia no islámica en la zona. Es

decididamente anti-occidental y anti-israelí.

2.1.2. SEGÚN EL TIPO DE BLANCOS

2.1.2.1. BLANCOS INSIGNIA

Este tipo de terrorismo no distingue relevancia nacional o internacional. Y dentro de los blancos insignia que se pueden mencionar; a los blancos **económicos**; como la Bolsa de Valores, las industrias, la aviación civil, el turismo. Otro tipo de blancos son los **militares**; como la defensa de las fronteras de los países, o por ejemplo el Pentágono en los Estados Unidos de América (como el ataque perpetrado el 11 de Septiembre). Sin embargo, también se toma en cuenta dentro de esta categoría a los blancos **psicológicos**, donde utilizando la aglutinación coyuntural de personas, como en estadios deportivos, discotecas, cines y otros, se amedrenta a personas cuya mayoría no tiene nada que ver con la estructura de un Estado.

2.1.2.2. BLANCOS REGIONALES

El terrorismo, utiliza blancos que poseen importancia regional dentro de una estructura estatal. Un ejemplo son los ataques terroristas perpetrados por el grupo ETA, que pretende la

consolidación de un País Vasco independiente dentro del territorio español.

2.2. DE ACUERDO AL MEDIO UTILIZADO

2.2.1. TERRORISMO BIOLOGICO (BIOTERRORISMO)

El Bioterrorismo, configurado como una forma que emplea el terrorismo para cumplir con sus objetivos. Utiliza armas biológicas para lograr su cometido; es decir, armas hechas con agentes infecciosos, como bacterias y virus, que provocan enfermedades humanas o plagas en los cultivos y en el ganado, con el fin de desestabilizar el orden constitucional de un Estado.

Algunos de los agentes que se prestan al uso como armas biológicas son los microorganismos vivientes, como las bacterias, los virus y las toxinas producidas por los propios microorganismos, plantas y animales. Algunos autores consideran a las toxinas como agentes químicos; sin embargo, en 1972 fueron incluidas dentro del listado de la Convención de Armas Biológicas. **([16])**

Este tipo de delitos, se encuentran tipificados dentro de los Delitos contra la Salud Pública en el Artículo 216, Inc. 2 del Código Penal. Sin embargo, si se contaminan alimentos, el riesgo de una infección masiva es aún mayor. Situación prevista en el mismo artículo, Inc. 3 del Código Sustantivo Penal.

[16] Internet Surf, Revista Electrónica, http://www.isurf.com.ar/98-06-junio/not_terr.htm

Según establece la Revista electrónica "Internet Surf", En 1991, un microbiólogo iraquí que escapó de su país tras la guerra del golfo Pérsico aseguró en una entrevista con un diario británico que en 1983 el gobierno de Bagdad ya estaba ensayando la guerra con agentes biológicos. Afirmando que ya había botulismo, salmonera y ántrax, señalando que "…Algunos amigos me dijeron, incluso, que se había descubierto la vía para hacer al ántrax mucho más nocivo. Yo lo que sé, es que experimentaron con clostridium botulinum tipo C (la fuente del botulismo). **([17])**

Este tipo de terrorismo, emplea a las armas biológicas, por varios motivos, entre los que podemos mencionar:

- Son económicas, ya que la toxina del botulismo puede producirse por apenas 400 dólares;
- Son fáciles de traficar;
- Es de muy difícil detección;
- No pueden ser captadas por los detectores de metales en los aeropuertos, por los rayos X o por perros entrenados, como sí pueden descubrirse las armas de fuego, las granadas y los explosivos plásticos;
- Son consideradas una vía efectiva para lograr el pánico en la población.

[17] Internet Surf, Rev. Cit.

- A diferencia de las armas químicas, necesitan sólo de su simiente para reproducir el agente en gran cantidad. Si la organización es lo suficientemente sofisticada, puede elaborar los virus que causan la viruela, el tifus y la fiebre amarilla. Las instrucciones para hacerlo libremente se encuentran en bibliotecas, libros, revistas y hasta en Internet.

Sobre los diferentes, virus, toxinas y otros, se puede mencionar como los más letales, al BOTULISMO y al ANTRAX.

El Botulismo, es la más peligrosa sustancia conocida y una severa y mortal amenaza como arma biológica. Un sólo gramo de este componente cristalino, dispersado por el aire, puede matar a 1 millón de personas. **([18])**

La manipulación de esta sustancia por terroristas, se denomina botulismo inhalatorio; el cuál genera una severa y simétrica parálisis fláccida descendente, que aparece luego de tres días del contagio.

Con respecto al Ántrax, se debe mencionar que, este es una bacteria (con esporas en forma de bastones), que vive en la tierra. Los seres humanos pueden infectarse don esta bacteria, mediante el contacto físico o la inhalación de sus esporas, que producen una toxina que puede ser fatal. El período de incubación es de 1 a 6 días, con síntomas de fiebre muy alta, fatiga y tos hasta que se

[18] http://www.guiadevacunacion.com.ar/notas/nota8.html

produce la muerte. El ántrax se previene con vacuna y se lo puede tratar a tiempo con antibióticos, incluyendo la penicilina.

Según el Secretario de Defensa estadounidense, William Cohen, el problema es que es relativamente fácil utilizarlo como arma y más fácil aún diseminarlo. Por lo que afirma que "La vacunación contra el ántrax es una segura y prudente medida de protección".**([19])**

2.2.2. TERRORISMO INFORMATICO (CIBERTERRORISMO)

El Ciberterrorismo, se configura como una novísima forma de practicar el terrorismo, empleando para ello, el uso de instrumentos informáticos, que permitan causar terror o zozobra en un territorio, determinado, para lograr desestabilizar el poder constituido en un Estado.

Se profundizará el tema del Terrorismo Informático de manera más puntual, en el Capitulo sexto de la presente Tesis.

2.3. TERRORISMO DE ESTADO

Entendemos al Terrorismo de Estado, como el uso sistemático por parte del gobierno de un Estado, de amenazas y represalias, con el fin de imponer obediencia y una colaboración activa a la población.

Los regímenes despóticos del pasado utilizaban con frecuencia prácticas de este tipo (como Bolivia durante varios

[19] www.nbc.med-org/anthraxinfo/Anthraxinfo3.html

gobiernos defectos), que las democracias modernas condenarían sin necesidad de realizar una crítica rigurosa.

Las formas más desarrolladas de Terrorismo de Estado, han sido los sistemas empleados en el siglo XX bajo el fascismo y el comunismo. Asimismo, la práctica de terror desde el poder se extendió en el siglo XX bajo regímenes militares o militarizados en el seno de democracias formales.

Estos regímenes totalitarios se caracterizaban por un monopolio de los medios de comunicación, la imposición de una ideología monolítica, la exigencia no sólo de obediencia sino de participación activa en las medidas policiales del Estado, y un aparato de policía secreta y de campos de concentración para disciplinar e incluso exterminar a los adversarios y disidentes. Los líderes potenciales de la oposición eran aislados, encarcelados, exiliados o asesinados.

Por lo general, los aparato represivo del Estado se extendía hasta fuera de sus fronteras y atacaban a enemigos que pertenecían a la población en el exilio, como fue el caso del asesinato de Liev Trotski en México a manos de agentes estalinistas; o la persecución política que se realizo en nuestro país durante los gobiernos de Hugo Banzer y García Meza.

El Terrorismo de Estado junto con sus aparatos paramilitares, es configurado como la mayor causa de violaciones a los derechos humanos en el continente. Un claro ejemplo es “La Operación Cóndor”, cuyo único objetivo real era viabilizar la represión violenta de las víctimas, configurándose en un proyecto personalmente ideado por el Coronel Manuel

Contreras (Cóndor I), siguiendo las órdenes de Augusto Pinochet, y otros responsables de países comprometidos, en esa época, en la lucha contra el Comunismo Internacional tales como Uruguay, Paraguay, Bolivia, Brasil y posteriormente Argentina.

"…La única autoridad que no teme es aquella que ha nacido del amor…Para que esta relación de miedo recíproco no exista entre hombres y gobierno, este debe ser reconocido y obedecido en libertad, con respeto y sincero amor. Al intervenir amenazas...surge el miedo: los hombres temen al gobierno, que los oprime, el gobierno tiene miedo de ellos, que podrían revelarse…" **([20])**

CAPITULO III

[20] FERRERO, Guglielmo, "The Principles of Power", Pág.35.

CONTEXTO INTERNACIONAL EN LA LUCHA CONTRA EL TERRORISMO

3.1. ORGANISMOS INTERNACIONALES

3.1.1. ORGANIZACIÓN DE LAS NACIONES UNIDAS (ONU)

La Organización de las Naciones Unidas, está convencida que los actos criminales con fines políticos concebidos o planeados para provocar un estado de terror en la población en general o en determinadas personas, son injustificables en todas las circunstancias, cualesquiera sean las consideraciones políticas, filosóficas, ideológicas, raciales, étnicas, religiosas o de cualquier otra índole que se hagan valer para justificarlos.

Además, Condena enérgicamente todos los actos, métodos y prácticas terroristas por considerarlos criminales e injustificables, dondequiera y por quienquiera sean cometidos.

La Organización de las Naciones Unidas, definiendo al problema del Terrorismo, dentro de sus preocupaciones como prioritario, ha delegado al Consejo de Seguridad, el establecer determinadas medidas que

se traducen en diferentes Resoluciones y Declaraciones, que logren la concientización de la población y sirvan como parámetro dentro de la creación de normas en los diferentes países del mundo. Sin embargo, no ha contemplado específicamente al Terrorismo Informático, dentro de las nuevas formas utilizadas para generar zozobra y terror en la población.

Sin embargo, se ha originado un compendio de Resoluciones y Declaraciones, que ameritan un breve análisis y se presentan de forma cronológica a continuación para un mejor entendimiento de la problemática que genera el Terrorismo en todas sus formas.

3.1.1.1. RESOLUCION 1368

De 12 de septiembre de 2001

Condena de los ataques terroristas perpetrados en los Estados Unidos

La presente Resolución, condena los actos de terrorismo que han causado inmensas pérdidas de vidas humanas, destrucción y daños en las ciudades de Nueva York (ciudad anfitriona de las Naciones Unidas) y Washington, D.C., así como en otros lugares.

Pero además de expresar sus condolencias y solidaridad con el pueblo y el

Gobierno de los Estados Unidos de América. Solicita urgentemente cooperación internacional para someter a la acción de la justicia a los autores, organizadores y patrocinadores de las atrocidades del 11 de septiembre de 2001. Y enfatiza que los colaboradores directos o indirectos de estos actos junto con los responsables de darles apoyo o asilo tendrán que rendir cuenta de sus hechos. Situación que se enmarca dentro del principio mencionado en el Capítulo I de la presente Tesis, referido al "No Home" y "No Finance".

3.1.1.2. RESOLUCIÓN 1373 de 28 De Septiembre de 2001 Consejo Seguridad Organización de Naciones Unidas sobre terrorismo. (Nuevas medidas para combatir terrorismo)

El Consejo de Seguridad aprobó por unanimidad una resolución que obliga a todos los estados miembros de la Organización de las Naciones Unidas (ONU), de la cuál Bolivia es parte, a aprobar una amplia serie de medidas para combatir el terrorismo.

En esta Resolución, la ONU a través del Consejo de Seguridad, se condena los

ataques terroristas ocurridos en Nueva York, Washington, D.C., y Pennsylvania del 11 de septiembre de 2001, y expresa su determinación de prevenir todos los actos de esa índole. Reafirmando asimismo que esos actos, al igual que todo acto de terrorismo internacional, constituyen una amenaza a la paz y la seguridad internacional. Pero además, hace mención al derecho de legítima defensa individual o colectiva, reconocido en la Carta de las Naciones Unidas y confirmado en la Resolución 1368 de 2001. Junto con la necesidad de luchar con todos los medios, de conformidad a la misma Carta, contra las amenazas a la paz y la seguridad internacional representada por los actos de terrorismo,

Esta Resolución, establece además que los Estados miembros, Impidan la circulación de terroristas o de grupos terroristas utilizando controles eficaces en frontera y controles de la emisión de documentos de identidad, pasaportes y visas. Empleando, la adopción de medidas para evitar la falsificación y la alteración ilegal. Situación que podría controlarse mediante la implementación de sistemas informáticos de seguridad, y adecuarse a un ataque Ciberterrorista.

3.1.1.3. RESOLUCIÓN 1377

De 12 de Noviembre de 2001

Declaración adjunta sobre los esfuerzos mundiales para combatir el terrorismo.

Resolución que establece que los actos de terrorismo internacional constituyen una de las amenazas más graves para la paz y la seguridad internacional en el siglo XXI, donde se deben enfrentar los nuevos desafíos; sin embargo, no establece que los nuevos desafíos, se presentan a través del avance tecnológico que es usado por los terroristas informáticos.

3.1.1.4. RESOLUCIÓN 1456

De 20 de Enero de 2003

Decide aprobar la declaración adjunta sobre la cuestión de la lucha contra el terrorismo.

Lo rescatable de esta Resolución, es que muy aparte de condenar al delito de Terrorismo, como sus antecesoras; señala que existe un peligro grave y cada vez mayor; como es el hecho de que los terroristas tengan acceso a materiales nucleares, químicos, biológicos, y otros potencialmente letales y, por consiguiente, es necesario hacer más estrictos los controles de esos materiales.

Sin embargo, recién en esta resolución, se menciona que en un mundo cada vez más globalizado se ha hecho más fácil para los terroristas explotar tecnologías, comunicaciones y recursos avanzados para sus objetivos criminales. Lo que nos da un parámetro para poder enfocar al Terrorismo Informático, ya que este tipo de terrorismo, utiliza a estas tecnologías y recursos avanzados.

3.1.1.5. CONVENIOS INTERNACIONALES

Si bien la Organización de las Naciones Unidas no logró concretar la elaboración de un tratado o convención de carácter general contra el terrorismo y más aún específico contra el Terrorismo Informático. Realizó un gran avance en lo que se refiere a instrumentos específicos y regionales. Logrando un compendio de 12 Convenios Internacionales; los cuáles son:

- El Convenio para la represión del apoderamiento ilícito de aeronaves, firmado en La Haya el 16 de diciembre de 1970;

- El Convenio para la represión de actos ilícitos contra la seguridad de la aviación

civil, firmado en Montreal el 23 de septiembre de 1971;

- La Convención sobre la prevención y el castigo de delitos contra personas internacionalmente protegidas, inclusive los agentes diplomáticos, aprobada por la Asamblea General de las Naciones Unidas el 14 de diciembre de 1973;

- La Convención Internacional contra la toma de rehenes, aprobada por la Asamblea General de las Naciones Unidas el 17 de diciembre de 1979;

- El Convenio sobre la protección física de los materiales nucleares, firmado en Viena el 3 de marzo de 1980;

- El Protocolo para la represión de actos ilícitos de violencia en los aeropuertos que prestan servicios a la aviación civil internacional, complementario del Convenio para la represión de actos ilícitos contra la seguridad de la aviación civil, firmado en Montreal el 24 de febrero de 1988;

- El Convenio para la represión de actos ilícitos contra la seguridad de la navegación marítima, hecho en Roma el 10 de marzo de 1988;

- El Protocolo para la represión de actos ilícitos contra la seguridad de las plataformas fijas emplazadas en la plataforma continental, hecho en Roma el 10 de marzo de 1988;

- El Convenio Internacional para la represión de los atentados terroristas cometidos con bombas, aprobado por la Asamblea General de las Naciones Unidas el 15 de diciembre de 1997;
- El Convenio Internacional para la represión de la financiación del terrorismo, aprobado por la Asamblea General de las Naciones Unidas el 9 de diciembre de 1999.

3.1.2. ORGANIZACIÓN DE LOS ESTADOS AMERICANOS (OEA)

3.1.2.1. CONVENCIÓN INTERAMERICANA CONTRA EL TERRORISMO

(Aprobada en la primera sesión plenaria celebrada el 3 de junio de 2002).

Esta Convención, se sujeta a los principios y disposiciones contenidos en la Carta de la Organización de los Estados Americanos y de la Carta de las Naciones Unidas. Ye en base a estos documentos, establece que el terrorismo constituye una

grave amenaza para los valores democráticos, la paz y la seguridad internacional. Y se configura en una profunda preocupación para todos los Estados Miembros.

La Convención Interamericana, establece que existen graves daños económicos a los Estados que pueden resultar de actos terroristas; lo que amerita la necesidad de la cooperación y la urgencia de los esfuerzos para erradicar el terrorismo.

Establece medidas para prevenir, combatir y erradicar el financiamiento del terrorismo. Contemplando la participación de los Estados miembros; donde cada uno de ellos deberá crear, un amplio régimen interno normativo y de supervisión para los bancos, otras instituciones financieras y otras entidades consideradas particularmente susceptibles de ser utilizadas para financiar actividades terroristas.

Estas medidas, establecidas por la Convención Interamericana contra el Terrorismo, permitirán un marco jurídico acorde al uso de nuevas tecnologías; ya que es bien sabido, que los movimientos transfronterizos utilizan sistemas informáticos que deben contar con un adecuado control para prevenir ataques Ciberterroristas.

3.1.2.2. CONVENCIÓN PARA PREVENIR Y SANCIONAR LOS ACTOS DE TERRORISMO CONFIGURADOS EN DELITOS CONTRA LAS PERSONAS Y LA EXTORSIÓN CONEXA CUANDO ESTOS TENGAN TRASCENDENCIA INTERNACIONAL

La presente Convención suscrita con los Estados miembros de los Estados Americanos; **([21])** ha considerado como base principal; la defensa de la libertad y de la justicia juntamente con el respeto de los derechos fundamentales de la persona, reconocidos por la Declaración Americana de Derechos y Deberes del Hombre y la Declaración Universal de los Derechos Humanos.

En su contenido, se puede observar la analogía en criterios básicos como lo son la prevención y sanción del delito de terrorismo. Y la exigencia a los Estados firmantes, en la creación de la normativa adecuada en pro de la lucha contra este delito.

Los Estados firmantes por su parte, deben prever las medidas a su alcance, en

[21] Suscrita en el Tercer Período Extraordinario de Sesiones de la Asamblea General, celebrada en Washington, DC, el 2 de febrero de 1971.

armonía con sus propias leyes, para impedir que en sus respectivos territorios se inicie la preparación de cualquier acto terrorista o que vayan a ser ejecutados en el territorio de otro Estado contratante.

Bolivia, es uno de los países signatarios, habiendo firmado en fecha 19 de diciembre de 2001, y depositando su ratificatoria el 8 de abril de 2002.

3.2. CONVENIOS INTERNACIONALES

3.2.1. CONVENIO DE GINEBRA - PARA LA PREVENCION Y REPRESION DEL TERRORISMO, DE 16 DE NOVIEMBRE DE 1937

El Convenio de Ginebra, fue creado por la Sociedad de las Naciones. El primer convenio fue suscrito por 24 Estados, pero solo ratificado por la India, y el segundo convenio fue firmado por 13 Estados pero no tuvo ninguna ratificación.

Bajo el título de "Protección de la población civil", el artículo 51 del Protocolo I codifica las normas fundamentales que han de respetarse en las operaciones militares. En el artículo 52, se añaden normas precisas que prohíben la destrucción de bienes de carácter civil, en particular los que forman parte de la infraestructura

civil **([22])**. En este artículo, encontramos asidero para proteger, fuera de nuestra legislación a la propiedad civil de aquellos perjudicados por los atentados Ciberterroristas.

3.2.2. CONVENCION EUROPEA PARA LA REPRESION DEL TERRORISMO, DE 1977.

Esta Convención, la primera regional europea; al igual que otras de su tipo, se basa en las anteriores similares ya dictadas. Como el Convenio para la Represión del Apoderamiento Ilícito de Aeronaves; el Convenio para la Represión de Actos ilícitos contra la Seguridad de la Aviación Civil y otros, donde se implique un ataque en contra de la vida, la integridad física o la libertad de personas civiles o internacionalmente protegidas (como los agentes diplomáticos).

3.2.3. CONVENCION DE LA ORGANIZACIÓN DE LA UNIDAD AFRICANA SOBRE LA PREVENCION Y LUCHA CONTRA EL TERRORISMO, DE 1999.

Es importante recordar el concepto de terrorismo que se contiene en la Convención africana, toda vez que es uno de los pocos instrumentos en el que se ha formulado una caracterización de ese delito.

[22] Al 30 de junio de 2002, 160 Estados eran Partes en el Protocolo I. Estados Unidos, Israel, Afganistán y algunos otros Estados, incluidos Irán, Irak y la República Democrática de Corea, no están vinculados por el Protocolo I, que prohíbe los ataques contra personas civiles y la infraestructura civil.

Acto terrorista significa:

a) "cualquier acto que constituya una violación de las leyes penales de un Estado Parte y que pueda poner en peligro la vida, la integridad física o libertad, o causar un grave daño o la muerte de cualquier persona, de un grupo de personas o causar daños a la propiedad, pública o privada, a los recursos naturales, al medio ambiente o al patrimonio cultural, así como la planificación e intento de:

i) intimidar, atemorizar, forzar, coercionar o inducir a cualquier gobierno, cuerpo, institución, al público en general o a cualquier segmento del mismo, para hacer o abstenerse de realizar cualquier acto, o para adoptar o abandonar un determinado punto de vista o para actuar de acuerdo con ciertos principios; o
ii) interrumpir cualquier servicio público, la entrega de cualquier servicio esencial para el público o crear una emergencia pública; o
iii) crear un insurrección general en un Estado.

b) cualquier promoción, auspicio, contribución para ejecución, ayuda, incitamiento, aliento, atentado, amenaza, conspiración, organización o procuramiento de cualquier persona, con la intención de cometer cualquier acto a los que se refiere el párrafo (a), incisos (i) al (iii)". **([23])**

[23] CONVENCION DE LA ORGANIZACIÓN DE LA UNIDAD AFRICANA SOBRE LA PREVENCION Y LUCHA CONTRA EL TERRORISMO, DE 1999.

3.2.4. CONVENCION DE LA ORGANIZACIÓN DE LA CONFERENCIA ISLÁMICA SOBRE LA LUCHA CONTRA EL TERRORISMO INTERNACIONAL, DE 1999.

La Organización de la Conferencia Islámica fue establecida en 1969 en Rabat (Marruecos). Entre los objetivos de la organización se encuentra el de trabajar para "cristalizar la unidad y expresar la solidaridad de la comunidad islámica (Ummah)".

Actúa representando los intereses y posturas de los estados islámicos a nivel mundial, de allí su gran importancia internacional.

Entre los considerandos de la Convención se puede encontrar la diferenciación entre "terrorismo" y "legítimo derecho a la ocupación extranjera". La Convención sostiene que: *"Confirmando la legitimidad del derecho de los pueblos a luchar contra la ocupación extranjera y contra regímenes racistas por todos los medios, incluyendo la lucha armada para liberar sus territorios y alcanzar el derecho a la autodeterminación e independencia de acuerdo con los propósitos y principios de la Carta y resoluciones de la Organización de Naciones Unidas".* **([24])**

[24] CONVENCION DE LA ORGANIZACIÓN DE LA CONFERENCIA ISLÁMICA SOBRE LA LUCHA CONTRA EL TERRORISMO INTERNACIONAL.

El artículo 2 de la convención señala: "*La lucha de los pueblos, incluyendo la lucha armada contra la ocupación extranjera, agresión, colonialismo y hegemonía, dirigida hacia la liberación y autodeterminación de acuerdo con el derecho internacional, no serán considerados como actos terroristas".***([25])**

Lo que resulta llamativo es que en esta misma parte de la Convención encontramos una frase que parecería contradecir la salvedad incluida en este texto con referencia al caso palestino: "*…convencidos de que el terrorismo no puede ser justificado de ningún modo, y que por consiguiente debe ser condenado en todas sus formas, manifestaciones, acciones, medios y prácticas, sin importar su origen, causa o propósito, incluyendo la participación directa o indirecta de los estados…".***([26])**

Con respecto a cuales hechos serán considerados como "actos terroristas", la Convención establece que deben ser las legislaciones internas de cada Estado las que determinarán esta cuestión en última instancia.

[25] Ibidem., Art. 2.
[26] CONVENCION DE LA ORGANIZACIÓN DE LA CONFERENCIA ISLÁMICA SOBRE LA LUCHA CONTRA EL TERRORISMO INTERNACIONAL.

CAPITULO IV

INTERNET

4.1. ANTECEDENTES

Aunque se pueda pensar que la Internet es algo que ha surgido en estos últimos tiempos, no es así: Internet ya lleva con nosotros unas cuantas décadas.

La Internet ha supuesto una revolución sin precedentes en el mundo de la informática y de las comunicaciones. Los inventos del telégrafo, teléfono, radio y ordenador sentaron las bases para esta integración de capacidades nunca antes vivida. Internet es a la vez una oportunidad de difusión mundial, un mecanismo de propagación de la información y un medio de colaboración e interacción entre los individuos y sus ordenadores independientemente de su localización geográfica.

La Internet representa uno de los ejemplos más exitosos de los beneficios de la inversión sostenida y del compromiso de investigación y desarrollo en infraestructuras informáticas. A raíz de la primitiva investigación en conmutación de paquetes, el gobierno, la industria y el mundo académico han sido copartícipes de la evolución y desarrollo de esta nueva y excitante tecnología. En la actualidad: www.cnn.com, www.eldiario.net ó juanperez@hotmail.com , son "palabras" comunes en el diario vivir.

4.1.1 PRIMER PERÍODO 1957- 1970 (NACIMIENTO)

En la Guerra Fría de (1957), la Unión Soviética lanza el Sputnik, el primer satélite artificial de comunicación. En respuesta a este hecho, Estados Unidos crea el ARPA. **([27])**

Los inicios de Internet nos remontan a los años 60. En plena guerra fría, Estados Unidos crea una red exclusivamente militar, con el objetivo de que, en el hipotético caso de un ataque ruso, se pudiera tener acceso a la información militar desde cualquier punto del país. Esta red se creó en 1969 y se llamó ARPANET.

En principio, la red contaba con 4 ordenadores distribuidos entre distintas universidades del país. Dos años después, ya contaba con unos 40 ordenadores conectados. Tanto fue el crecimiento de la red que su sistema de comunicación se quedó obsoleto. Entonces dos investigadores crearon el Protocolo TCP/IP, que se convirtió en el estándar de comunicaciones dentro de las redes informáticas.

ARPANET siguió creciendo y abriéndose al mundo, y cualquier persona con fines académicos o de investigación podía tener acceso a la red. Las funciones militares se desligaron de ARPANET y fueron a parar a MILNET, una nueva red creada por los Estados Unidos. La NSF (National Science Fundation) crea su propia red informática llamada NSFNET, que más tarde absorbe a

[27] ARPA, Organismo de Proyectos de Investigación Avanzada, que se configuraría más adelante en un sistema digital, lo que hoy es la Internet.

ARPANET, creando así una gran red con propósitos científicos y académicos. El desarrollo de las redes fue abismal, y se crean nuevas redes de libre acceso que más tarde se unen a NSFNET, formando el embrión de lo que hoy conocemos como INTERNET. **([28])**

4.1.2. SEGUNDO PERÍODO: 1970-1990 (DEL EJÉRCITO A LA UNIVERSIDAD)

Fueron las Universidades estadounidenses, responsables en gran medida del desarrollo de ARPANET.

Vint Cerf y Bob Kahn especifican el diseño del Programa de Control de Transmisión (TCP) y se utiliza por primera vez el término Internet.

En 1983 se adoptó el TCP/IP como estándar principal para todas las comunicaciones, y en 1990 desapareció ARPANET para dar paso junto a otras redes TCP/IP a Internet. Por aquel entonces también comenzaron a operar organizaciones privadas en la Red. **([29])**

De 1980 a 1985, se desarrolla el Sistema de Denominación de Dominios (Domain Name System), **([30])** que sirve para identificar a las páginas Web de cada persona, organización o institución; por ejemplo: www.cocacola.com , dominio que pertenece a la mundialmente conocida Coca Cola Company.

[28] www.mundoinformatico.ar/hist_internet_pa667/
[29] www.mundoinformatico.ar/hist_internet_pa668/
[30] Ibidem.

4.1.3. TERCER PERIODO 1990-1995 (EXPANSIÓN)

Esta expansión se mantiene fuera de los ámbitos militares y de las universidades, ya que en 1990-91, Tim Berners-Lee, inventa la World Wide Web, el elemento que más ha contribuido a popularizar Internet. **([31])**

En 1994, se difunde la versión comercial del navegador Netscape Navigator. Software de aplicación que permite navegar por la Internet. **([32])**

Nace el buscador de información, programas, música y otros: Yahoo, que es considerado (así como Google), uno de los más visitados.

4.1.4. CUARTO PERIODO, 1996- 2004 (MULTIMEDIA-CIENTOS DE MILLONES DE USUARIOS)

En este periodo, debido al éxito consolidado en las conexiones a nivel mundial al Internet. Empresas comerciales como la Microsoft, empieza una lucha sin cuartel, con el fin de monopolizar el programa de acceso a Internet; por lo que incluye en su Sistema Operativo (Windows), al Internet Explorer. Situación que le llevo a grandes juicios que buscaban lograr que estos 2 programas se vendan por separado; lo que daría un mayor mercado al Netscape Navegator por ejemplo.

[31] www.noticiasdot.com/publicaciones/2004/0904/0109/noticias010904/noticias010904-19.htm
[32] Ibidem.

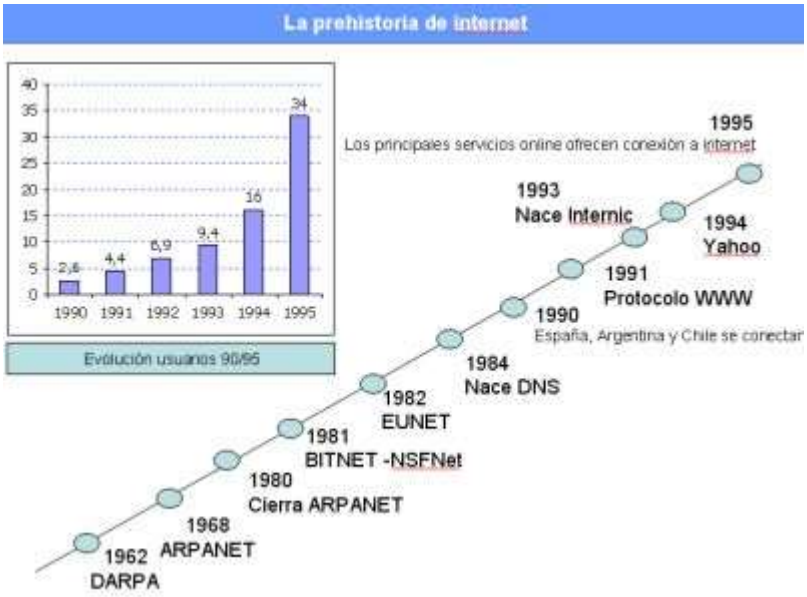
Se produjo la inclusión de contenidos multimedia (sonido, video, animación e interactividad), junto con la técnica de streaming para la transmisión fluida de vídeo, usada en las Videoconferencias.

En 1999, el formato de sonido MP3 **([33])**, desestabiliza a las multinacionales de la discografía. Ya para el año 2002, se contabilizan aproximadamente, 500 millones de usuarios en el mundo. **([34])**

Actualmente es casi imposible calcular los sitios Web que existen y los servidores a los que tenemos acceso. Internet se ha desarrollado en esta última década mucho, y en parte es debido a los fines comerciales de las empresas. Internet ya no es la red de investigación; ni la red militar para lo que fue creada, ahora Internet es, ante todo, un negocio, y eso ha sido lo que ha empujado su desarrollo.

33 MP3, Método de compresión de música, manteniendo su calidad pero ocupando un menor tamaño. (300 canciones aproximadamente en un disco compacto).

34 www.noticiasdot.com/publicaciones/2004/0904/0109/noticias010904/noticias010904-19.htm.



Cuadro 1: Prehistoria de Internet **([35])**

4.2. CONCEPTO

Internet, es la abreviación de dos palabras inglesas: interconnected Network (redes interconectadas).

La conexión de dos o más computadoras entre sí; constituyen una red. Ahora bien, estas redes, a su vez, pueden conectarse con otras de mayor o menor número de computadoras.

Imaginemos, cuántas redes entonces, existen en Bolivia; pero vamos a un más lejos; pongámonos a pensar, cuántas redes existirán en todo el mundo.

4.3. FUNCIONAMIENTO

[35] www.noticiasdot.com/publicaciones/2004/0904/0109/noticias010904/noticias010904-19.htm

En Internet, las comunicaciones concretas se establecen entre dos puntos: uno es el ordenador personal desde el que usted accede y el otro es cualquiera de los servidores que hay en la Red y facilitan información.

El fundamento de Internet es el TCP/IP, un protocolo de transmisión que asigna a cada máquina que se conecta un número específico, llamado "número IP" (que actúa a modo de "número teléfono único") como por ejemplo 192.555.26.11.

El protocolo TCP/IP sirve para establecer una comunicación entre dos puntos remotos mediante el envío de información en paquetes. Al transmitir un mensaje o una página con imágenes, por ejemplo, el bloque completo de datos se divide en pequeños bloques que viajan de un punto a otro de la red, entre dos números IP determinados, siguiendo cualquiera de las posibles rutas. La información viaja por muchos ordenadores intermedios a modo de repetidores hasta alcanzar su destino, lugar en el que todos los paquetes se reúnen, reordenan y convierten en la información original. Millones de comunicaciones se establecen entre puntos distintos cada día, pasando por cientos de ordenadores intermedios.

4.4. CONEXION

Generalmente se accede a Internet a través de la línea telefónica, pero también es posible hacerlo mediante un cable de fibra óptica.

En el caso de la línea telefónica, se debe utilizar un MODEM, (aparato electrónico que modula y remodula datos) el cuál una vez conectado a la computadora, cumple la función de recibir y enviar los datos utilizando la infraestructura telefónica de la ciudad (por medio de sus postes y cables), para conectarse a un servidor que posteriormente conduzca a la Internet.

Si se requiere una conexión más veloz, se deberá utilizar una conexión ADSL, que ya no utiliza a la infraestructura telefónica para conectarse a la Internet; sino más bien, utiliza una red de fibra óptica, lo que permite mayor estabilidad y velocidad en la conexión.

4.5. UTILIDADES

La aplicación de la tecnología en la era de la información, desencadena la aparición de diversos usos que se puede encontrar en el sus herramientas, donde una de ellas, tal vez la más poderosa; es la Internet. De estos usos mencionados, se hará referencia a los más destacados:

4.5.1. BUSQUEDA DE INFORMACION

La búsqueda de cualquier tipo de información, se realiza mediante los "motores de búsqueda". En estos se guarda información de miles de millones de sitios y sus bases de datos permiten la búsqueda rápida de información. Existen varios motores entre ellos los más

importantes son: www.google.com , www.yahoo.com , www.altavista.com y otros.

Estos mecanismos están diseñados para que, con solo escribir una palabra o un conjunto de ellas y hacer "clic" **([36])**, aparezca en la computadora, muchísima de la información que se consigue en el mundo sobre cualquier temática.

4.5.2. CHAT

Chat es una palabra en ingles cuya traducción significa conversar, pero a esta altura se convirtió en un término específico para designar el encuentro entre dos o más personas en Internet que mantienen una conversación en tiempo real. Para chatear basta con tener una PC, con conexión a Internet, elegir un apodo (nick name) e ingresar en alguna sala de Chat.

El chat fue evolucionando y paso desde los precarios BBS (Bulletin Board System, una de las formas más primitivas de establecer conexiones entre computadoras) a los universos virtuales, que incluyen audio y video. En poco tiempo se convirtió en una verdadera pasión de multitudes.

4.5.3. VIDEOCONFERENCIA

[36] CLIC, - Palabra que refiere el pulsar algún botón del Mouse.

Consiste en una charla a distancia, que incluye sonido y video; utilizando una Webcam **([37])** y naturalmente una conexión a la Internet.

Es necesario tener una placa multimedia, un software de videoconferencia, un micrófono, parlantes y la cámara.

4.5.4. CORREO ELECTRONICO

El correo electrónico (e-mail) es tal vez el principal servicio de Internet, y sin duda el de mayor importancia histórica. Cada persona que está conectada cuenta con un "buzón electrónico" personal, simbolizado en una dirección de correo: esos nombres con la letra arroba (@) que usted habrá visto en revistas, tarjetas de visita y anuncios. El buzón de correo electrónico sirve para enviar y recibir mensajes a otros usuarios, y por eso no hay nunca dos nombres iguales.

La primera parte de una dirección identifica habitualmente a la persona y la segunda a la empresa u organización para la que trabaja, o al proveedor de Internet a través del que recibe la información. Así, una dirección como juanperez@facultaddederecho.umsa.edu identificaría, imaginariamente, a un usuario que se llamara Juan Pérez, cuyo buzón estuviera (@ significa en inglés "at", es decir, "en") en un ordenador llamado facultaddederecho, en la Universidad Mayor de San

[37] Cámara de video diseñada para ser conectada a una computadora.

Andrés, y que está, es un centro universitario (.edu). El correo electrónico permite enviar texto o archivos codificados como texto, generalmente de pequeño tamaño (gráficos u hojas de cálculo, por ejemplo).

Gracias al Correo Electrónico, se pueden enviar mensajes a varias personas, responderlos de forma automática, guardar listas personales de direcciones y de grupos de colaboradores. También funcionan listas automáticas de correo entre grupos que comparten un interés especial (como series de televisión, aficiones comunes o proyectos en grupo).

Quizás la única desventaja que vale la pena mencionar es que pueden incorporarse a los mensajes, una variedad de virus que van desde simples mensajes no deseados, hasta daños en el hardware del computador. Sin embargo, la utilización de un buen antivirus, soluciona el problema en un 90 %.

CAPITULO V
DELINCUENCIA INFORMATICA

5.1. EL DELITO

Para poder enfocar a la delincuencia informática; es preciso primeramente tener una idea clara de lo que representa el delito en sí. De tal forma, es que rescatamos las definiciones expresadas por reconocidos jurisconsultos en el ámbito penal en el contexto internacional y nacional.

Edmundo Mezger, define al delito como "una acción típicamente antijurídica y culpable, a la que está señalada una pena" **([38])**. Por su parte, Von Liszt, señala que el delito se puede definir como "el acto culpable contrario al derecho y sancionado con una pena". **([39])**

Dentro de la bibliografía nacional, encontramos los criterios del eminente jurisconsulto, Dr. Fernando Villamor Lucía, quién señala que el delito en términos generales es "toda conducta descrita por la ley penal cuya consecuencia es la pena o las medidas preventivas o represivas". **([40])**

[38] Mezger, Edmundo, Derecho Penal, Parte General, Pág. 328.
[39] VON LISTZ, Franz, Tratado de Derecho Penal, traducción por Luís Jiménez de Asúa, Pág. 265.
[40] VILLAMOR, Lucia Fernando, Derecho Penal Boliviano, Parte General, Tomo I, Pág. 61.

Algo que se debe destacar, es que el Código Penal boliviano de 1834, definía al delito y al delincuente; señalando que "Comete delito el que libre y voluntariamente y con malicia, hace u omite lo que la ley prohíbe o manda bajo alguna pena. En toda infracción libre de la ley, se entenderá haber voluntad y malicia, mientras que el infractor no pruebe o no resultare claramente lo contrario" **([41])**, definición que según Villamor, establecía la presunción de culpabilidad del encausado. Sin embargo, la Constitución Política del Estado con su reforma en 1967, deroga este principio y establece el de la presunción de la inocencia mientras no se pruebe lo contrario.

El Código Penal vigente, elevado a Ley de la República por Ley Nº 1768 "Ley de Modificaciones al Código Penal" de 11 de marzo de 1997; no define al delito, resaltando el hecho de que la tarea de definirlo, no compete al legislador; teoría defendida por el moderno derecho penal.

Por todo lo expuesto anteriormente, se puede definir al delito, como toda acción típicamente antijurídica y culpable, que es merecedora de una sanción penal.

De tal forma se establece que los elementos del delito son: la acción, la tipicidad, la antijuricidad y la culpabilidad que involucra a la imputabilidad que como consecuencia encuentra a la sanción.

[41] CÓDIGO PENAL BOLIVIANO de 1834, Artículo 1.

5.2. DELITO INFORMÁTICO

A los delitos informáticos se les denomina de diferentes maneras: delitos relacionados con las computadoras, crimen por computadora, delitos electrónicos y computer crime entre otros.

El delito informático, implica actividades criminales que durante el transcurso del tiempo, han tratado de ser consideradas por los diferentes países, como figuras típicas de carácter tradicional, tales como robo, hurto, fraudes, falsificaciones, perjuicios, estafas, sabotaje, etc. Sin embargo, debe destacarse que el uso de las distintas técnicas informáticas ha creado nuevas posibilidades del uso indebido de las computadoras, lo que ha generado a su vez, la necesidad de regulación por parte del Derecho.

Tiedemann, señala que el delito informático, "es cualquier acción ilegal en la que el ordenador sea el instrumento o el objeto del delito y, más concretamente cualquier delito ligado al tratamiento automático de datos". **([42])**

Por su parte, Parker, considera más conveniente ampliar el concepto hasta comprender cualquier forma abusiva del empleo de herramientas informáticas. En este contexto, define a delito informático como "cualquier acto criminoso relacionado con la tecnología informática, por el cuál una víctima ha sufrido una pérdida y un autor, ha obtenido intencionalmente una ganancia" **([43])**.

[42] TIEDEMANN, Aspects Criminologiques de la Delinquance d' Affaires", Pág 231.
[43] Parker, Crime By Computer, Pág 86.

Jijena Leiva, define al Delito Informático, como "toda acción típica, antijurídica y culpable, para cuya consumación se usa la tecnología computacional o se afecta a la información contenida en un sistema de tratamiento automatizado de la misma" **([44])**.

Por otro lado, Maria de la Luz Lima, señala que el delito informático se configura desde un sentido amplio "como cualquier conducta criminógena o criminal que en su realización hace uso de la tecnología electrónica ya sea como método, medio o fin" **([45])**.

Por los conceptos señalados anteriormente, se puede establecer que el delito informático es toda acción típica, antijurídica y culpable merecedora de una sanción, que emplea a los medios informáticos como medio, método o fin, en la comisión del delito.

5.2.1. BIEN JURIDICO PROTEGIDO

La aparición de las Nuevas Tecnologías en la Sociedad ha obligado a la creación de nuevos tipos penales que sancionen las conductas ilícitas realizadas por los nuevos medios de transmisión de información.

[44] Estractado de Levene, Ricardo y Chiavalloti, Delitos Informáticos, VI Congreso Iberoamericano de Derecho e Informática.
[45] Lima de La Luz, María, Delitos Electrónicos, México, Academia Mexicana de Ciencias Penales, Pág. 100.

Asimismo cabe indicar que el fenómeno de los delitos informáticos encuentra en la **"Información"** el bien jurídico que se encuentra protegido.

5.2.2. ELEMENTO OBJETIVO

El elemento objetivo, que caracteriza al delito informático en su manifestación más común, es todo atentado que signifique dañar o desviar el correcto desempeño de la computadora con la finalidad de causar un perjuicio que redunde en el beneficio material o moral para sí o para otro.

En algunos casos la acción tiende a afectar elementos componentes de la computadora, como lo son el Hardware o el Software. Sin embargo en otros casos, la computadora es utilizada como medio o instrumento para cometer el delito. También es posible que, sin afectar los componentes de una computadora ni inutilizarla para la perpetración de un hecho ilícito; lo ilegal de la conducta, consista en el uso indebido de un computador sin la autorización respectiva.

5.2.3. ELEMENTO SUBJETIVO

El elemento subjetivo, está constituido por el dolo o la culpa con que actúa el sujeto activo del delito informático.

5.2.4. SUJETO ACTIVO

El delincuente, por lo general se encuadra en el modelo de persona de un determinado nivel de inteligencia y educación superior al común. Sin embargo, ocurre algo irónicamente contrario a lo referido, ya que existe un número elevado de personas que se convierten en delincuentes informáticos, por culpa. Es decir, que cometen la figura delictiva sin la intención de hacerlo. (El caso de niños, que acceden a páginas y vulneran sistemas de seguridad entre otros).

Por otro lado, algunas de las personas que pueden cometer delitos informáticos, pueden ser: los operadores de sistemas, cuando modifican, agregan, sustituyen o eliminan información o determinados programas, o los copian para distribuirlos y obtener beneficios económicos; los crackers **([46])**, que rompen el sistema de seguridad de determinado programa o sistema informático, para modificar o destruir el contenido, obteniendo de tal forma réditos económicos a gran magnitud; los supervisores de sistemas, ya que estos conocen en integridad el acceso y las falencias del sistema informático a su cargo, situación que les permite tener un acceso mayor al medio computacional.

5.2.5. SUJETO PASIVO

El sujeto pasivo, es la víctima del delincuente informático; por lo general, son los bancos y entidades financieras, por la creciente utilización de las transferencias de fondos de forma electrónica, donde

[46] Para mayor referencia sobre los Crackers, véase el punto 5.4. del presente capítulo.

circulan grandes cantidades de dinero. Sin embargo, el sujeto pasivo, puede ser cualquier persona que sienta la vulneración de sus derechos de propiedad y confidencialidad.

5.2.6. CLASIFICACION DE LOS DELITOS INFORMATICOS

Es evidente la variedad de clasificaciones que existen sobre los delitos informáticos; sin embargo, para determinar un mejor ámbito de trabajo y una clasificación estándar, es que en la presente Tesis, se utilizará la clasificación que la Organización de las Naciones Unidas ha establecido, para ser utilizada como marco, dentro de la normativa de los Estados miembros.

5.2.6.1. FRAUDES COMETIDOS MEDIANTE MANIPULACIÓN DE COMPUTADORAS

5.2.6.1.1. MANIPULACIÓN DE DATOS DE ENTRADA

Este tipo de fraude informático, conocido también como sustracción de datos, representa el delito informático más común ya que es fácil de cometer y difícil de descubrir.

Este delito no requiere de conocimientos técnicos de informática y puede realizarlo

cualquier persona que tenga acceso a las funciones normales de procesamiento de datos en la fase de adquisición de los mismos.

5.2.6.1.2. MANIPULACIÓN DE PROGRAMAS

Es muy difícil de descubrir y a menudo pasa inadvertida debido a que el delincuente debe tener conocimientos técnicos concretos de informática. Este delito consiste en modificar los programas existentes en el sistema de computadoras o en insertar nuevos programas o nuevas rutinas. Un método común utilizado es el denominado "Caballo de Troya", que consiste en insertar instrucciones de computadora de forma encubierta en un programa informático para que pueda realizar una función no autorizada al mismo tiempo que su función normal.

5.2.6.1.3. MANIPULACIÓN DE DATOS DE SALIDA

Se efectúa fijando un objetivo al funcionamiento del sistema informático. El ejemplo más común

es el fraude de que se hace objeto a los cajeros automáticos mediante la falsificación de instrucciones para la computadora en la fase de adquisición de datos. Tradicionalmente esos fraudes se hacían a base de tarjetas bancarias robadas; sin embargo, en la actualidad se usan ampliamente equipo y programas de computadora especializados para codificar información electrónica falsificada en las bandas magnéticas de las tarjetas bancarias y de las tarjetas de crédito.

5.2.6.1.4. MANIPULACIÓN INFORMÁTICA APROVECHANDO REPETICIONES AUTOMÁTICAS DE LOS PROCESOS DE CÓMPUTO

Es una técnica especializada que se denomina "técnica del salchichón" o técnica del "salami", en la que "rodajas muy finas" apenas perceptibles, de transacciones financieras, se van sacando repetidamente de una cuenta y se transfieren a otra. (Es el caso de los centavos que se

redondean en las transacciones bancarias)

5.2.6.1.5. FALSIFICACIONES INFORMÁTICAS

Utilizadas como objeto, cuando se alteran datos de los documentos almacenados en la computadora. Y como instrumento, siendo que las computadoras pueden utilizarse también para efectuar falsificaciones de documentos de uso comercial. Con el uso de fotocopiadoras computarizadas a base de rayos láser y con la ayuda de escaners, que copian documentos originales, los cuáles son alterados posteriormente mediante programas de diseño gráfico computarizado.

5.2.6.2. DAÑOS O MODIFICACIONES DE PROGRAMAS O DATOS COMPUTARIZADOS

5.2.6.2.1. SABOTAJE INFORMÁTICO

Es el acto de borrar, suprimir o modificar sin autorización funciones o datos de computadora con intención de obstaculizar el funcionamiento normal del sistema. Las técnicas que permiten cometer sabotajes informáticos son los virus informáticos, los gusanos

informáticos y las bombas lógicas o cronológicas.

5.2.6.3 ACCESO NO AUTORIZADO A SERVICIOS Y SISTEMAS INFORMÁTICOS

Situación que puede darse por motivos diversos: desde la simple curiosidad, como en el caso de muchos piratas informáticos (hackers) hasta el sabotaje o espionaje informático.

5.2.6.3.1. PIRATAS INFORMÁTICOS

El acceso se efectúa a menudo desde un lugar exterior, situado en la red de telecomunicaciones, recurriendo a uno de los diversos medios que se mencionan a continuación. El delincuente puede aprovechar la falta de rigor de las medidas de seguridad para obtener acceso o puede descubrir deficiencias en las medidas vigentes de seguridad o en los procedimientos del sistema. A menudo, los piratas informáticos se hacen pasar por usuarios legítimos del sistema; esto suele suceder con frecuencia en los sistemas en los que los usuarios pueden emplear contraseñas comunes o

contraseñas de mantenimiento que están en el propio sistema.

5.2.6.3.1. REPRODUCCIÓN DESAUTORIZADA DE PROGRAMAS INFORMÁTICOS CON PROTECCIÓN LEGAL

Esta puede significar una pérdida económica sustancial para los propietarios legítimos. Algunas jurisdicciones han tipificado como delito esta clase de actividad y la han sometido a sanciones penales. Como es el caso de Bolivia, donde existe el Decreto Supremo Nº 24582 de 25 de Abril de 1997. Reglamento de Soporte Lógico o Software**,** que contempla la protección de los derechos de autor sobre el soporte lógico y los bancos de datos.

El problema ha alcanzado dimensiones transnacionales con el tráfico de esas reproducciones no autorizadas a través de las redes de telecomunicaciones modernas. Al respecto, la consideración de la presente Tesis, es que la reproducción no autorizada de programas informáticos no es un delito informático

debido a que el bien jurídico a tutelar es la propiedad intelectual.

5.2.7. EL DELITO INFORMATICO EN LA LEGISLACION NACIONAL

Nuestro ordenamiento jurídico, se encuentra desprovisto, de la normativa penal adecuada para la sanción eficaz del delito de terrorismo a través de sus diferentes formas; sin embargo, se han incluido algunas referencias normativas dentro de los diferentes cuerpos legales vigentes.

El **Código Penal boliviano, en su Título XII, Delitos contra la propiedad, señala en el capítulo XII**, concretamente en el **Artículo 363º. Bis. a la MANIPULACIÓN INFORMÁTICA**; estableciendo que "…el que con la intención de obtener un beneficio indebido para sí o un tercero, manipule un procesamiento o transferencia de datos informáticos que conduzca a un resultado incorrecto o evite un proceso tal cuyo resultado habría sido correcto, ocasionando de esta manera una transferencia patrimonial en perjuicio de tercero, será sancionado con reclusión de uno a cinco años y con multa de sesenta a doscientos días…". ([47])

A si mismo, el **Artículo 363º. Ter. sobre ALTERACIÓN, ACCESO Y USO INDEBIDO DE DATOS INFORMÁTICOS),** del mismo cuerpo legal, establece que : "…el que sin estar autorizado se apodere, acceda,

[47] Código Penal Boliviano. Art. 363 bis.

utilice, modifique, suprima o inutilice, datos almacenados en una computadora o en cualquier soporte informático, ocasionando perjuicio al titular de la información, será sancionado con prestación de trabajo hasta un año o multa hasta doscientos días…". **([48])**

Por lo que se puede ver que, primeramente no se establece una definición exacta de delito informático; y si bien se da una sanción por la manipulación y el acceso no autorizado a datos para un beneficio personal, está claro que la comisión de otros tipos penales vía medios informáticos se encuentra desprovista de sanción, por lo que seguramente, se adecuarán a los tipos clásicos de estafa, hurto, delitos financieros y otros tipificados en nuestra normativa. Situación que debería ser atendida por los legisladores, con la creación de una Ley que contemple exclusivamente a los delitos informáticos.

Por otro lado, se debe señalar, que existe el **Decreto Supremo Nº 24582 de 25 de Abril de 1997. Reglamento de Soporte Lógico o Software,** que contempla fuera de algunas definiciones; la protección de los derechos de autor sobre el soporte lógico y los bancos de datos, que con características de individualidad y originalidad surgen y se exteriorizan en una forma de expresión susceptible de ser reproducida e incorporada en un soporte informático. Que junto con la **Ley Nº 1322 de 13 de Abril de 1992, Ley de**

[48] Código Penal Boliviano, Art. 363 ter.

derechos de Autor; protege los bienes intelectuales, sean estos plasmados en un soporte lógico o exclusivamente la forma literaria plástica o sonora, mediante la cual las ideas del autor son descritas, explicadas, ilustradas o incorporadas en las obras literarias, científicas o artísticas, como lo señala la Ley de Derechos de Autor mencionada.

5.2.8. EL DELITO INFORMATICO EN LA LEGISLACION INTERNACIONAL

5.2.8.1. ESTADOS UNIDOS.

Este país adoptó en 1994 el "Acta Federal de Abuso Computacional" (18 U.S.C. Sec.1030), que modificó al "Acta de Fraude y Abuso Computacional" de 1986, con la finalidad de eliminar los argumentos técnicos acerca de qué es y que no es un virus, un gusano, un caballo de Troya y en que difieren de los virus, la nueva acta proscribe la transmisión de un programa, información, códigos o comandos que causan daños a la computadora, a los sistemas informáticos, a las redes, información, datos o programas (18 U.S.C.: Sec. 1030 (a) (5) (A). La nueva ley es un adelanto porque está directamente en contra de los actos de transmisión de virus.

El Acta de 1994 diferencia el tratamiento a aquellos que de manera imprudencial lanzan ataques de virus de aquellos que lo realizan con la intención de hacer estragos. Definiendo dos niveles para el tratamiento de quienes crean virus:

a) "Para los que intencionalmente causan un daño por la transmisión de un virus, el castigo de hasta 10 años en prisión federal más una multa; y
b) Para los que lo transmiten sólo de manera imprudencial la sanción fluctúa entre una multa y un año en prisión". **([49])**

La nueva ley constituye un acercamiento más responsable al creciente problema de los virus informáticos, específicamente no definiendo a los virus sino describiendo el acto para dar cabida en un futuro a la nueva era de ataques tecnológicos a los sistemas informáticos en cualquier forma en que se realicen. Diferenciando los niveles de delitos, la nueva ley da lugar a que se contemple qué se debe entender como acto delictivo.

Asimismo, en materia de estafas electrónicas, defraudaciones y otros actos dolosos relacionados con los dispositivos de

[49] Acta Federal de Abuso Computacional

acceso a sistemas informáticos, la legislación estadounidense sanciona con pena de prisión y multa, a la persona que defraude a otro mediante la utilización de una computadora o red informática.

5.2.8.2. ALEMANIA.

Este país sancionó en 1986 la Ley contra la Criminalidad Económica, que contempla los siguientes delitos:

- Espionaje de datos.
- Estafa informática.
- Alteración de datos.
- Sabotaje informático.

5.2.8.3. AUSTRIA.

La Ley de reforma del Código Penal, sancionada el 22 de Diciembre de 1987, en el artículo 148 sanciona a aquellos que con dolo causen un perjuicio patrimonial a un tercero influyendo en el resultado de una elaboración de datos automática a través de la confección del programa, por la introducción, cancelación o alteración de datos o por actuar sobre el curso del procesamiento de datos. Además contempla sanciones para quienes comenten este hecho utilizando su profesión de especialistas en sistemas.

5.2.8.4. GRAN BRETAÑA.

Debido a un caso de hacking en 1991, comenzó a regir en este país la "Computer Misuse Act" (Ley de Abusos Informáticos). Mediante esta ley el intento, exitoso o no, de alterar datos informáticos es penado con hasta cinco años de prisión o multas.

Esta ley tiene un apartado que específica la modificación de datos sin autorización. Los virus están incluidos en esa categoría. El liberar un virus tiene penas desde un mes a cinco años, dependiendo del daño que causen.

5.2.8.5. HOLANDA.

El 1º de Marzo de 1993 entró en vigencia la Ley de Delitos Informáticos, en la cual se penaliza el hacking, el phracking, la ingeniería social (arte de convencer a la gente de entregar información que en circunstancias normales no entregaría), y la distribución de virus.

La distribución de virus está penada de distinta forma si se escaparon por error o si fueron liberados para causar daño.

Si se demuestra que el virus se escapó por error, la pena no superará el mes de prisión; pero, si se comprueba que fueron liberados con la intención de causar daño, la pena puede llegar hasta los cuatro años de prisión.

5.2.8.6. FRANCIA.

En enero de 1988, este país dictó la Ley relativa al fraude informático, la cual prevé penas de dos meses a dos años de prisión y multas de diez mil a cien mil francos por la intromisión fraudulenta que suprima o modifique datos.

Asimismo, esta ley establece una sanción en su Artículo 462 inc. 3, por la conducta intencional y a sabiendas de estar vulnerando los derechos de terceros que haya impedido o alterado el funcionamiento de un sistema de procesamiento automatizado de datos. Por su parte el Artículo 462-4 también incluye en su tipo penal una conducta intencional y a sabiendas de estar vulnerando los derechos de terceros, en forma directa o indirecta, haya introducido datos en un sistema de procesamiento automatizado o haya suprimido o modificado los datos que éste

contiene, o sus modos de procesamiento o de transmisión.

También la legislación francesa establece un tipo doloso y pena el mero acceso, agravando la pena cuando resultare la supresión o modificación de datos contenidos en el sistema, o bien en la alteración del funcionamiento del sistema (sabotaje).

Por último, esta ley en su artículo 462 inciso 2, sanciona tanto el acceso al sistema como al que se mantenga en él y aumenta la pena correspondiente si de ese acceso resulta la supresión o modificación de los datos contenidos en el sistema o resulta la alteración del funcionamiento del sistema.

5.2.8.7. ESPAÑA.

En el Nuevo Código Penal de España, el Artículo 263 sanciona al que causare daños en propiedad ajena. En tanto, el artículo 264-2 establece que se aplicará la pena de prisión de uno a tres años y multa a quien por cualquier medio destruya, altere, inutilice o de cualquier otro modo dañe los datos, programas o documentos electrónicos ajenos contenidos en redes, soportes o sistemas informáticos.

Este nuevo Código Penal de España sanciona en forma detallada esta categoría delictual (Violación de secretos, Espionaje, Divulgación), aplicando pena de prisión y multa, agravándolas cuando existe una intención dolosa y cuando el hecho es cometido por parte funcionarios públicos se penaliza con inhabilitación.

5.2.8.8. CHILE.

Chile fue el primer país latinoamericano en sancionar una Ley contra delitos informáticos, la cual entró en vigencia el 7 de junio de 1993.

Según esta ley, la destrucción o inutilización de los de los datos contenidos dentro de una computadora es castigada con penas desde un año y medio a cinco años de prisión. Asimismo, dentro de esas consideraciones se encuentran los virus.

Esta ley prevé en el Art. 1º, el tipo legal vigente de una conducta maliciosa tendiente a la destrucción o inutilización de un sistema de tratamiento de información o de sus partes componentes o que dicha conducta impida, obstaculice o modifique su funcionamiento. En tanto, el Art. 3º tipifica

la conducta maliciosa que altere, dañe o destruya los datos contenidos en un sistema de tratamiento de información.

5.3. HACKERS

Hacker deriva de hack, que significa hachar en ingles. Con este termino se describía inicialmente la manera en la cual los técnicos telefónicos arreglaban cajas defectuosas; el bueno y viejo golpe seco.

En 1959 la denominación alcanzó a los estudiantes del Massachussets Institute of Technology (El famoso MIT de los Estados Unidos), cuando ante una falla de la computadora valvular IBM 407, incluían el casero método del impacto o golpe de costado para lograr solucionar problemas esotéricos de dichos equipos. **([50])**

No fue hasta septiembre de 1970 donde John Draper descubre que el silbato que acompañaba de obsequio a las cajas de cereal "Capitán Crunch", duplicaba la frecuencia de tono de 2600 hz. permitiéndole hacer llamadas telefónicas gratis. A partir de este hecho, una organización denominada YIP se encargó de difundir este hecho, logrando así que la gente hablara de forma gratuita por teléfono. Con esto el YIP intentaba boicotear el financiamiento gubernamental a la guerra

[50] http://www.el-mundo.es/navegante/2003/12/26/seguridad/1072431321.html

de Vietnam, al tiempo que perjudicaba a la compañía telefónica AT&T. **([51])**

Lo señalado anteriormente, permite concluir que se entiende por Hackers, a un Experto en programación y códigos, que disfruta con la exploración de detalles de los sistemas y aprovecha los recursos y posibilidades que éste le brinda. Así como también a un Experto que utiliza sus habilidades en sistemas de información para acceder a retos en forma no autorizada.

En el New Hacker's Dictionary **([52])** (Nuevo diccionario del hacker), se describe a los hackers como personas inteligentes, intelectuales, los cuáles se interesan en cualquier sujeto que les pueda proveer estimulación mental y reconoce que el objetivo de sus colegas es hackear por hackear, y su verdadero estímulo es el desafío intelectual de superar limitaciones.

Es hacker la persona capaz de explorar un sistema hasta sus lugares más recónditos, en busca del conocimiento. Es aquel que no se conforma con lo obvio, que tiene una visión de las cosas que pasa desapercibida al resto de mortales

Por todo lo expuesto, en esta Tesis se afirma que los Hackers realizan sus acciones por diversión, a diferencia de los Ciberterroristas que operan para presionar a un gobierno para lograr desestabilizarlo.

5.3.1. CRONOLOGIA DE LOS HECHOS MÁS DESTACADOS

[51] http://www.el-mundo.es/navegante/2003/12/26/seguridad/1072431321.html
[52] New Hacker's Dictionary, Eric Raymond.

La siguiente cronología fue extractada de "The Hacker Crackdown" (La Caza de Hackers) **([53])**, obra literaria electrónica que goza del derecho "freeware". **([54])**

1865	- Se funda el Servicio Secreto de Estados Unidos (USSS).
1876	- Alexander Graham Bell inventa el teléfono.
1878	- Las autoridades, enfurecidas, expulsan por primera vez a unos chavales del sistema telefónico.
1939	- Redada del Servicio Secreto contra *Los Futuristas*, un grupo de aficionados a la ciencia-ficción.
1971	- Los *Yippies*, un grupo de *phreaks*, empiezan a publicar la revista 'YIPL/TAP'.
1972	- La revista 'Ramparts' es confiscada por un escándalo de estafa con *cajas azules.*
1978	- Ward Christenson y Randy Suess crean la primera BBS (Bulletin Board System).
1982	- William Gibson acuña el término *ciberespacio*.
1982	- Redada contra el grupo *414 Gang*.
1983	- AT&T es desmantelada y convertida en varias empresas.
1984	- El Congreso aprueba el «Acta de Control Global de Delitos», dando al USSS, jurisdicción sobre los delitos con tarjetas de crédito y los delitos informáticos.

[53] The Hacker Crackdown, Bruce Sterling, Freeware literario, traducida al castellano por el Equipo de Traductores de Criptópolis, Pág. 10 a la 12.

[54] Freeware, "Parte libre", documento electrónico, es decir que su uso puede ser incorporado en cualquier otro trabajo, siempre y cuando se mencione a los autores y no se haga ninguna modificación al texto.

1984	- Se crea el grupo *Legion of Doom*.
1984	- Se funda la publicación '2600: The Hacker Quarterly'.
1984	- Publicado el 'Whole Earth Software Catalog'.
1985	- Primer *pinchazo* policial en una BBS.
1985	Comienza a funcionar el Enlace Electrónico Planetario (WELL).
1986	- Aprobada el «Acta de Fraudes y Delitos Informáticos».
1986	- Aprobada el «Acta de Privacidad de las Comunicaciones Electrónicas».
1987	- Agentes de Chicago forman la Brigada de Fraudes y Delitos Informáticos.
1988	- Julio. El Servicio Secreto graba con cámaras ocultas el encuentro de *hackers* «SummerCon».
1988	- Septiembre. *Prophet* asalta la red de computadoras AIMSX de BellSouth y descarga a su computadora y a Jolnet el *documento E911*.
1988	- Septiembre. El Departamento de Seguridad de AT&T es informado de la acción de *Prophet*.
1988	- Octubre. El Departamento de Seguridad de Bellcore es informado de la acción de *Prophet*.
1989	- Enero. *Prophet* le envía a *Knight Lightning* el *documento E911*.
1989	- 25 de febrero. *Knight Lightning* publica el *documento E911* en la revista electrónica *PHRACK*.
1989	- Mayo. La Brigada de Chicago registra la casa de *Kyrie* y la detiene.
1989	- Junio. El grupo *NuPrometheus League* distribuye *software* propiedad de Apple Computer.

1989	- 13 de junio. La oficina del Estado de Florida encargada de los presos en libertad condicional, es conectada a una línea de sexo telefónico al ser alterada una centralita.
1989	- Julio. El Servicio Secreto y la Brigada de Fraudes y Delitos Informáticos de Chicago registran la casa de *Fry Guy*.
1989	- Julio. El Servicio Secreto registra las casas de *Prophet*, *Leftist* y *Urvile*, en Georgia.
1990.	- 15 de enero. La *caída del sistema* del Día de Martin Luther King deja inoperativa la red de larga distancia de AT&T en todo el país.
1990	- 18 y 19 de enero. La Brigada de Chicago registra la casa de *Knight Lightning* en Saint Louis.
1990	- 24 de enero. El Servicio Secreto y la Policía del Estado de Nueva York registran las casas de *Phiber Optik*, *Acid Phreak* y *Scorpion*, en Nueva York.
1990	- 1 de febrero. El Servicio Secreto registra la casa de *Terminus* en Maryland.
1990	- 3 de febrero. La Brigada de Chicago registra la casa de Richard Andrews.
1990	- 6 de febrero. La Brigada de Chicago registra la oficina de Richard Andrews.
1990	- 6 de febrero. El Servicio Secreto arresta a *Terminus*, *Prophet*, *Leftist* y *Urvile*.
1990	- 9 de febrero. La Brigada de Chicago arresta a *Knight Lightning*.
1990	- 20 de febrero. El Departamento de Seguridad de AT&T desconecta la computadora de acceso público «Attctc» de Dallas.
1990	- 21 de febrero. La Brigada de Chicago registra la casa de Robert Izenberg en Austin.

1990	- 1 de marzo. La Brigada de Chicago registra las oficinas de Steve Jackson Games, Inc., y las casas de *The Mentor* y *Erik Bloodaxe*, en Austin.
1990	- 7, 8 y 9 de mayo. El Servicio Secreto y el Departamento de Crimen Organizado de Arizona llevan a cabo, dentro de la «Operación Sundevil», registros en Cincinatti, Detroit, Los Angeles, Miami, Newark, Phoenix, Pittsburgh, Richmond, Tucson, San Diego, San Jose y San Francisco.
1990	Mayo. El FBI interroga a John Perry Barlow sobre el caso *NuPrometheus*.
1990	Junio. *Mitch* Kapor y Barlow, fundan la Electronic Frontier Foundation; Barlow publica el manifiesto 'Crimen y Desconcierto'.
1990	- 24 a 27 de julio. Juicio de *Knight Lightning*.
1991	- Febrero. Mesa redonda de CPSR en Washington D.C.
1991	- 25 a 28 de marzo. Conferencia «Computadoras, Libertad y Privacidad», en San Francisco.
1991	- 1 de mayo. La Electronic Frontier Foundation, Steve Jackson y otros, emprenden acciones legales contra los miembros de la Brigada de Chicago.
1991	- 1 y 2 de julio. Una caída del *software* de las centralitas, afecta a Washington, Los Angeles, Pittsburgh y San Francisco.
1991	- 17 de septiembre. Una *caída del sistema* telefónico de AT&T afecta a Nueva York y a tres aeropuertos.

Cuadro 2: The Hacker Crackdown Bruce Sterling

5.4. CRACKERS

El término ingles crack, significa romper, quebrar, rajar o descifrar (en términos informáticos); por lo que se define al Cracker, como aquél delincuente informático que rompe un sistema para lograr un beneficio meramente personal.

El Cracker diseña y fabrica programas de guerra y hardware para destruir el software y a las comunicaciones como por ejemplo, los sistemas telefónicos, el correo electrónico o el control de otros ordenadores remotos. Muchos Crackers "cuelgan" **([55])** paginas Web por diversión o envían a la red su ultima creación de algún virus polimórfico. **([56])**

También existen Crackers que se dedican a crear Cracks **([57])** para Software importantes y una que los fabrican, negocian con ellos.

Los crackers tienden a agruparse en grupos pequeños, secretos y privados, a diferencia de los hackers que desarrollan comunidades abiertas para intercambiar, discutir y colaborar con su trabajo.

Los mismos crackers, pueden usar herramientas (software) hechas por ellos mismos o por otros crackers, que les sirven para desencriptar **([58])** información, "romper" los passwords **([59])** de las computadoras, e incluso de los programas y compresores de archivos; aunque si estos programas no son manejados por malas manos, pueden ser muy útiles para los técnicos o para uno mismo.

[55] Cuelgan, es decir, saturan el sistema informático para que este ya no pueda funcionar conforme a su diseño, logrando pararlo.
[56] Virus que cambia de forma, para no ser detectado.
[57] Rutinas de programación que activan las restricciones de un Software, logrando habilitar todas sus funciones sin tener que pagar por él.
[58] Lograr romper la clave que protege al programa manipulaciones no autorizadas.
[59] Contraseñas, que el dueño de la información o programa introduce para salvaguardar sus datos.

Por otro lado, los crackers, pueden ser empleados rencorosos o frustrados de alguna compañía, que tengan fines maliciosos o de venganza en contra de alguna empresa o persona, o pueden ser estudiantes que quieran demostrar sus habilidades pero de la manera equivocada o simplemente personas que lo hagan solo por diversión, pero a diferencia de los Hackers, estos dañan inclusive irremediablemente a los sistemas informáticos.

Finalmente, se debe señalar que todos los Terroristas Informáticos, son considerados Crackers, ya que rompen cualquier medio de protección que posea el Sistema Informático; claro está, añadiendo el propósito de desestabilizar el orden constitucional de un Estado.

5.5. PHRACKERS

El Phracker es una persona que con amplios conocimientos de telefonía, puede llegar a realizar actividades no autorizadas con los teléfonos, por lo general celulares. Construyen equipos electrónicos artesanales que pueden interceptar y hasta ejecutar llamadas de aparatos telefónicos celulares sin que el titular se percate de ello.

Este tipo de delincuente informático, concentra su atención en el "pinchado" de líneas telefónicas; logrando espiar llamadas y lograr información para determinados objetivos.

El terrorista informático, puede además de considerarse un Cracker, ser un Phracker, ya que necesita conseguir información esencial, antes de perpetrar sus atentados; por lo

que el espiar, llamadas telefónicas, se constituye en una buena herramienta para estos delincuentes.

Lamentablemente, en la Internet se distribuyen planos con las instrucciones y nomenclaturas de los componentes necesarios para construir diversos modelos de aparatos que sirven para el "pinchado" y "clonación" de líneas telefónicas.

5.6. LAMERS

Un Lamer es simple y sencillamente un "tonto" de la informática, una persona que se siente Hacker por haber bajado de Internet el algún programa que permita ingresar a otro sistema informático; alguien a quien le guste bajar virus de la red e instalarlos en la PC de sus amigos, aunque mas bien podría decírsele como un Cracker de pésima calidad; en general alguien que cree que tiene muchos conocimientos de informática y programación, pero no tiene ni la más mínima idea de ello.

Los Lamers, son considerados los usuarios más detestables, dentro del ciberespacio, ya que no poseen capacidad de innovación y de creación; conformándose con enseñar a quienes no tienen mucho conocimiento informático, logros ajenos.

CAPITULO VI

TERRORISMO INFORMATICO (CIBERTERRORISMO – CYBERTERRORISM)

6.1. ANTECEDENTES

El terrorismo informático, es identificado en 1976 por Andy Marshall, alto funcionario del Pentágono de los EEUU, quien le dio el nombre de INFOGUERRA (Guerra de la información), ya que sostenía que este tipo de terrorismo, utilizaba bytes en lugar de balas, causando daños a infraestructura e inclusive originaba la muerte de civiles y militares. Situación que más adelante sería develada por Alvin Toffler, quién en 1996 predecía el **"Electronic Perl Harbor"**, ataque que abarcaría a todo el planeta en cuestión de minutos.

El ataque terrorista puede producirse en cualquier momento y de forma secuencial; es decir, que no existe una hora, ni fecha determinada, pero sí podría existir una cadena de ataques originados en distintos sitios geográficos, enfocándose en un mismo objetivo, y en reiteradas oportunidades por lapsos de tiempo calculados de acuerdo al daño que se quiera causar.

6.2. CONCEPTO

El Ciberterrorismo se identifica con el avance tecnológico que día a día estamos experimentando a nivel mundial; ya que son necesarios medios informáticos para su ejecución, y estos se mejoran cada vez más en capacidad de almacenamiento de información, miniaturización y velocidad.

Este tipo de terrorismo, reconoce como principal canal de ataque a la red Internet (Interconnected Network); servicio, que esta disponible en todo el mundo y de fácil acceso ya que no infiere gastos económicos elevados, por lo que fácilmente se puede conseguir un servicio de conexión las 24 horas del día y en distintos lugares geográficos a bajo costo y sin muchas preguntas.

El terrorista informático utiliza pocos recursos para lograr su objetivo; emplea por lo general un computador personal, un Modem y una conexión a Internet.

Desde el punto de vista del Derecho Penal, el terrorismo se manifiesta mediante la ejecución repetida de delitos por los cuales se crea un estado de alarma o temor en la colectividad o en ciertos grupos sociales o políticos. Es entonces evidente que

la sociedad debe defenderse y entonces el Estado crea las figuras penales que reprimen esta clase de hechos.

Por lo que se puede definir al Terrorismo Informático, como la sucesión de actos para infundir terror utilizando medios informáticos, con el fin de lograr un cambio radical en el orden constitucional de un Estado.

Pero la pregunta surge, ¿Cómo se puede causar tanto daño (inclusive la muerte) con tan pocos medios?. Y la respuesta, es que si bien el terrorista utiliza estos medios básicos para lograr su cometido; encuentra otros medios y herramientas dentro de la red.

La mayoría de las universidades de prestigio a nivel mundial, cuentan con sistemas informáticos de gran capacidad y alta velocidad en el tratamiento y transmisión de datos, debido a la gran cantidad de alumnos que tiene y por ende a la afluencia de solicitudes de todo tipo que se le hace vía la Internet. Situación que es aprovechada por los Ciberterroristas, ya que acceden a estos sistemas y los utilizan como plataformas virtuales de ataque contra determinado objetivo.

Pero no solamente existen servidores de gran capacidad y velocidad en Universidades, sino también en bibliotecas, centros de experimentación y desarrollo tecnológico, centros médicos, oficinas gubernamentales de control de estadísticas poblacionales, etc. Lo que facilita al Ciberterrorista variar en cuanto a la elección de la plataforma virtual de ataque. Sin embargo, se debe señalar que el Ciberterrorista, no solo utiliza

Servidores de última tecnología, sino también servidores de tecnología elemental como los que utilizan la mayoría de los países, donde se incluye a Bolivia.

Es decir, que la tecnología ya existe, no hace falta un arsenal, ni poseer computadoras sofisticadas para cometer actos de terrorismo informático; el terrorista informático solo necesita tener el conocimiento y la habilidad suficiente para utilizar estos medios (ajenos), y utilizarlos como armas potenciales de destrucción.

El Terrorismo Informático es una figura heterogénea, pues puede revestir formas muy distintas de delitos, aunque predominan los que van contra las personas eligiendo la víctima entre jefes de Estado, ministros, muchedumbres, etc.

De tal forma, es que con la aparición de nuevas tecnologías, como la Internet; el terrorismo utiliza a los medios informáticos para ejecutar sus actividades delincuenciales, configurándose así el Terrorismo Informático o Ciberterrorismo.

6.3. CARACTERÍSTICAS

"…Obtener cien victorias en cien batallas no es el culmen de la excelencia. Sojuzgar al ejército oponente sin luchar es la cima de la excelencia…". **([60])**

Hoy, las palabras de El Arte de la Guerra, vertidas al papel hace más de 2.000 años por Sun Tzu, aparecen dotadas de una vigencia extraordinaria.

[60] SUNT ZU, El Arte de la Guerra.

Internet ha tornado en realidad el sueño del guerrero: vencer sin combatir, controlar al enemigo sin exponerse uno mismo. La innovación imparable en tecnologías de la información y las comunicaciones, especialmente las basadas en las computadoras y el Internet, han creado el potencial de una nueva forma de hacer la guerra en la era de la información; donde aparece una nueva forma de terrorismo configurado en el Terrorismo Informático, que presenta las siguientes características :

6.3.1. ASIMETRÍA POLÍTICA – ESTRATEGICA

El Diccionario de la Real Academia de la Lengua, establece que asimetría es "…la falta de correspondencia exacta en forma, tamaño y posición de las partes de un todo…". **([61])**

Dentro de una definición aplicada al campo militar; se entiende por asimetría; a la diferencia logística, de capacidades y de defensa entre dos contendores.

El Terrorismo Informático, presenta como una de sus características principales, a la asimetría política – estratégica, que consiste en el empleo de los mejores métodos no militares para lograr una ventaja militar.

Esta situación, desemboca en una clara ventaja que poseen los terroristas informáticos con respecto a los medios de defensa militar de un país; ya que esta defensa se basa en el combate que utiliza armamentos

[61] Diccionario de la Real Academia de la Lengua, 19º Ed.

convencionales en tierra, cielo y mar. Dejando a un lado el armamento lógico; que es empleado por este tipo de criminales.

Además, surge la posibilidad de que se presenten dificultades en la toma de decisiones que permitan prevenir un ataque terrorista que utilice medios informáticos; ya que existirán enormes dificultades para distinguir un ataque de Terrorismo Informático con otro tipo de actividades y eventos tales como espionaje, accidentes, falla de sistemas y acciones de los "hackers". La incapacidad de efectuar tales distinciones puede llevar a respuestas militares muy cautelosas ante reales situaciones de crisis.

6.3.2. NUEVO CAMPO DE BATALLA (CYBERWAR)

El Terrorismo Informático, incorpora a los tradicionales espacios de ataque (tierra, aire y mar), un nuevo y poco controlado sitio para realizar sus ataques; el ciberespacio.

El ciberespacio no tiene fronteras, razón por la cuál, no es extraño que el este se haya convertido en un terreno de lucha social y que las relaciones entre la sociedad real y la virtual sean profundamente contradictorias.

6.3.3. BAJOS RECURSOS Y ALTO RIESGO

El Ciberterrorismo se constituye en una forma de terrorismo que emplea un alto riesgo y bajo costo, al alcance de las Naciones pobres.

Bajos costos de inversión; en comparación con los altos costos de las fuerzas estratégicas. Un ataque terrorista informático, puede ser efectuado sin necesidad de recurrir a un gran financiamiento y además, por cualquier individuo u organización.

6.3.4. DIFÍCIL LOCALIZACIÓN

Debido a que el ataque terrorista, es perpetrado utilizando la Internet; al ser una red tan grande y distribuida por todo el mundo, la localización exacta del ataque, es realmente una tarea muy difícil. Sin embargo, se debe señalar, que una forma de identificación es la dirección IP que cada computadora posee; dirección que es diferente en cada ordenador.

Sin embargo, la existencia de hosts que ocultan la identidad del remitente, convirtiendo el mensaje en anónimo ha podido ser aprovechado por grupos terroristas para remitirse consignas y planes de actuación internacional.

La escasez de un sistema de inteligencia y las vulnerabilidades de la guerra de información no son bien comprendidas. Puede que la identidad de los posibles adversarios no sea conocida y los métodos clásicos de recolección y análisis de inteligencia no sean aplicables. Se

deberá desarrollar nuevos métodos de análisis y de relaciones entre organizaciones.

6.3.5. PLATAFORMA CIBERNÉTICA

Para poder entender lo que es una Plataforma Cibernética, primeramente se debe definir a la "cibernética".

El diccionario de la Real Academia de la Lengua, define a cibernética como "…el Estudio de las analogías entre los sistemas de control y comunicación de los seres vivos y los de las máquinas; y en particular, el de las aplicaciones de los mecanismos de regulación biológica a la tecnología…". **([62])**

Además conceptuada como una ciencia interdisciplinaria que trata de los sistemas de comunicación y control en los organismos vivos, las máquinas y las organizaciones. El término cibernética, que proviene del griego kybernēeēs ('timonel' o 'gobernador'), fue aplicado por primera vez en 1948 por el matemático estadounidense Norbert Wiener a la teoría de los mecanismos de control. En pocas palabras; cibernética es la relación hombre – máquina. **([63])**

Una de las características del Terrorismo Informático, es la utilización de Plataformas Cibernéticas;

[62] Diccionario de la Real Academia de la Lengua, 19º Ed.
[63] Diccionario de la Real Academia de la Lengua, 19º Ed.

es decir un espacio virtual donde se genera el ataque terrorista.

Por ejemplo, el ataque, aparentemente se realiza en un determinado lugar geográfico del planeta, digamos Israel; sin embargo, se ha ejecutado desde otro lugar totalmente remoto al que se piensa como puede ser Japón. A esta figura se denomina plataforma cibernética o Plataforma Virtual.

6.4. FORMAS DE ATAQUE

No es un secreto que existe vulnerabilidades internas dentro de cada Estado. La economía y la sociedad actual están descansando cada vez más en una infraestructura de redes de información de alto rendimiento en todo aspecto, desde vuelos comerciales y distribución de electricidad hasta la administración de cuentas bancarias personales; se encuentran a merced de un especialista informático.

Tomemos como ejemplo al piloto de un cazabombardero F-117. A medida que mueve los controles, genera señales electrónicas que activan las superficies de control del avión. Sin embargo, el F-117 es una plataforma inherentemente inestable que requiere constante corrección para mantenerse en el aire. Estas correcciones se hacen automáticamente, muchas veces por segundo, basadas en la información brindada por los sensores que monitorean la altitud del avión, la velocidad, etc. El piloto no puede reaccionar lo suficientemente rápido como para brindar la información necesaria para mantener el avión

en el aire; en lugar de esto, lo que él ingresa es información adicional necesaria para que el avión pueda volar hacia donde él quiere ir. El paso siguiente en la evolución de la interconexión hombre-máquina (que es lo que en la actualidad está buscando la Fuerza Aérea de Estados Unidos), sería ir más allá de los requisitos de la reacción física, tomando los impulsos eléctricos directamente del cerebro y utilizando estos impulsos como órdenes para un sistema de control manejado por computadora.

Se puede señalar, otro tipo el ataque mediante la distorsión de información en cuanto a la ubicación del enemigo utilizando GPRS. Es decir, que el Terrorista Informático, cambia la ubicación del enemigo alterando vía satélite la información, consiguiendo que se ataque no al enemigo sino a alguna aldea con civiles inocentes.

En 1998, El departamento de protección al Ambiente de EEUU, envió por correo electrónico los datos de desastres químicos y las vulnerabilidades de este departamento, por ende de todo el país. Situación que podía haber sido aprovechada por los Ciberterroristas para introducir agentes químicos. **([64])**

6.4.1. HIGH TECH (ALTA TECNOLOGÍA)

Este tipo de ataque, causa daños en los sistemas informáticos que controlan equipos electrónicos de los cuales depende el funcionamiento de diferentes

[64] www.computerworld.com

"servicios críticos", como los han llamado en Estados Unidos (agua, luz, etc.).

La perpetración de ataques Ciberterroristas High Tech, más que solamente lograr la atención de la población, buscan la muerte de la población. **([65])**

Estos ataques, se han clasificado de la siguiente manera:

6.4.1.1. INTERRUPCION

El terrorista informático, una vez infiltrado en el sistema informático, destruye un recurso del sistema, o lo vuelve no disponible. Por ejemplo logra la destrucción del elemento hardware, como el disco duro; corta la línea de comunicación o deshabilita el sistema de gestión de ficheros. **([66])**

Howard Schmidt, consejero informático de la Casa Blanca señala que "los incidentes relacionados con la informática están creciendo en número, sofisticación, gravedad y coste"… "Nos estamos enfocando en las armas de destrucción masiva, pero tenemos que tener muy en cuenta las armas de interrupción masiva de servicios que existen en el ciberespacio"… "El problema lo pueden

[65] Véase el inciso 6.5. de la presente tesis "Tipos de Ataque".
[66] Lo que hace inservible al Sistema Informático.

provocar tanto grandes organizaciones como pequeños adolescentes creadores de virus, el terrorismo informático no tiene fronteras". **([67])**

6.4.1.2. INTERCEPCIÓN

Se produce cuando el sujeto activo consigue el acceso a un determinado recurso y afecta a la confidencialidad de datos. Un ejemplo es el pinchar una línea para conseguir datos que se encuentren en el Internet; copia ilícita de programas, etc.

En este tipo de ataque, es donde la presencia de los phrackers es requerida.

6.4.1.3. MODIFICACIÓN

El Terrorista Informático en esta ocasión no solo ha ingresado al sistema informático; sino también es capaz de modificarlo (ataque contra la integridad). Logrando el cambio de los valores de un archivo que contenga determinados datos; alteración de programas para que funcionen de forma diferente o la modificación de los mensajes que se envían por la Internet.

6.4.1.4. FABRICACIÓN

[67] Terrorismo Informático Golpea Economía Mundial, Artículo, http://www.24horas.com.pe/tecnologia/1035228287.php

El Terrorismo Informático, ataca insertando objetos falsificados en el sistema informático (ataque contra la autenticidad).

Este tipo de ataque se puede dividir en 2:

6.4.1.4.1. ATAQUES PASIVOS

Donde el Ciberterrorista no altera la comunicación; solamente escucha y monitoriza para lograr información que le sea útil para perpetrar sus actos. Pero además de obtener datos importantes, controla el tráfico y la frecuencia de las comunicaciones.

Los datos que interesan al terrorista informático son: el origen y el destino de la comunicación; las horas habituales de intercambio de datos entre los que se comunican, logrando establecer los periodos de actividad.

Estos ataques pasivos son difíciles de detectar; debido a que no provocan alteración en los

datos. Sin embargo, se pueden evitar mediante la encriptación de los mismos.

6.4.1.4.1. ACTAQUES ACTIVOS

A diferencia de los pasivos; este tipo de ataques involucran la modificación de los datos, creando un falso flujo de información para lograr la confusión en el objetivo. Esta categoría de ataques pueden dividirse en:

a) SUPLANTACION DE IDENTIDAD

El Ciberterrorista se infiltra en el sistema con una identidad diferente. Por ejemplo, las secuencias de autentificación de ingreso pueden ser capturadas y repetidas; logrando el ingreso a recursos restringidos, tal cuál sería el robo de una contraseña.

b) REACTUACIÓN

Es decir, una doble actuación. Donde uno o varios mensajes o instrucciones legítimas son capturados y

repetidos para lograr un efecto diferente al normal. Ejemplo, el ingreso de dinero en forma repetida a una determinada cuenta. Esta es una forma de conseguir financiamiento para las actividades terroristas.

Aquí, se puede observar que se comete el delito tipificado por la Organización de las Naciones Unidas, como la "Técnica del Salchichón", o del "Salami", mencionada en el capítulo V, punto 5.2.5.1 Fraudes Cometidos Mediante Manipulación De Computadoras, inciso D).

c) MODIFICACIÓN DE MENSAJES

Utilizado normalmente para modificar una parte de un determinado mensaje legítimo; reordenación y retardo de los mensajes, logrando un efecto no autorizado. Un ejemplo es que en lugar de que el mensaje diga "ingrese 1000 $us. a la

cuenta **A**" dirá "ingrese 1000 $us. a la cuenta **B**".

d) DEGRADACIÓN FRAUDULENTA DEL SERVICIO

Ataque que no permite el uso normal de los recursos informáticos y de toda comunicación. Se presenta tal situación, en el momento que el Ciberterrorista suprime todos los mensajes que estén dirigidos a una determinada entidad. O por el contrario satura el sistema de esta entidad, enviando mensajes diferentes en forma repetida. **([68])**

6.4.1.5. SPOOFING (ENVIO DE SEÑALES FALSAS)

El Spoofing es el envío de señales falsas. Se puede efectuar mediante el envío de una señal electromagnética pero también, suplantando una fuente de entrada para desbaratar un sistema de información.

[68] Este tipo de mensajes repetidos a una sola entidad, también se conoce como la "denegación de servicio (Dos)", que será contemplado en el inciso "G" del presente numeral.

6.4.1.6. ESTEGANOGRAFIA

Etimológicamente la expresión Esteganografía viene del griego *stèganos,* equivalente a escondido y *gràfein* que significa escribir; concepto que a su vez indica secreto, recóndito, reservado. Es un secreto muy reservado y de importancia. Entendido también como un misterio, cosa oculta y muy difícil de conocer. **([69])**

Según una noticia publicada por el diario estadounidense "Usa Today" "…Osama Bin Laden es un experto informático en criptografía, ya que el multimillonario saudí utiliza técnicas de Esteganografía, que le permiten ocultar y encriptar mensajes en cualquier tipo de archivo, de manera que una simple imagen puede contener mensajes ocultos para sus comandos terroristas…". **([70])** El director de la CIA, George Tenet, ya había advertido en febrero del 2003, ante un comité del Senado estadounidense que había terroristas que utilizaban la Internet y otros recursos de tecnología para comunicar mensajes secretos.

6.4.1.7. DoS

[69] Diccionario de la Real Academia de la Lengua, 19º ed.
[70] IBLNEWS / TECNOLOGÍA, Los atentados contra Estados Unidos obligan a una revisión de la seguridad, http://iblnews.com/news/print.php3?id=21123

(ATAQUES DE NEGACION DE SERVICIO)

Los ataques de Denegación de Servicio (Denial of Service, DoS) son uno de los estratos más básicos de la seguridad informática y de los que más difícil es estar a salvo. Consisten en enviar mucha información a una máquina, en forma de cartas electrónicas (el llamado 'mailbombing') o paquetes de datos, hasta que ésta no lo soporta y deja de funcionar. Pura fuerza bruta donde gana quien tiene más "ancho de banda" **([71])** para lanzar contra el otro.

Definitivamente, este es un tipo de ataque utilizado comúnmente por los Terroristas Informáticos; un claro ejemplo es el atentado que sufrió la página en inglés de la cadena de noticias árabe Al-Jazira, que fue víctima de un ataque Ciberterrorista, junto con el crítico sitio canadiense Yellowtimes.org se encontraron, entre las primeras víctimas de un ataque cibernético en el presente año.

6.4.1.8. PHISHING

"Phishing" es el término usado por los piratas informáticos cuyos métodos tienen como objetivo conseguir información financiera y las contraseñas de los usuarios mediante

[71] A mayor ancho de banda, más velocidad en la conexión a la Internet.

engaños, correos con direcciones falsificadas y duplicación ilícita de sitios legales online.

6.4.2. LOW TECH (BAJA TECNOLOGÍA)

Los ataques "Low Tech" o de baja tecnología, consisten básicamente en actos de propaganda sobre la ideología, fundamento y los fines de los terroristas informáticos.

El medio que estos delincuentes utilizan para promover sus actos; es el cambio sin autorización del contenido de las páginas Web; normalmente institucionales y representativas de algún ente gubernamental.

Pero se debe mencionar, que si bien la motivación en este ataque de baja tecnología, busca el manifestar la existencia de los grupos terroristas e informar sobre sus atentados provocando zozobra en la población. Esta agresión (aparentemente leve), genera confusión en la información que la gente maneja, y puede desencadenar un desequilibrio en el sistema económico, político y social de un Estado. Un ejemplo podría manifestarse, cuando se informa erróneamente sobre la estabilidad de la Banca en un determinado País; generando una baja en los depósitos bancarios y un retiro de fondos masivo.

Se podría mencionar, el caso de Malasia, donde los terroristas informáticos, eliminaron toda la información de la página parlamentaria de ese país.

Otros ejemplos de estos casos se pueden encontrar en nuestro vecino Perú, donde las páginas en Internet de la Oficina Nacional de Procesos Electorales (ONPE) y del Jurado Nacional de Elecciones del Perú (JNE) fueron retiradas sorpresivamente del ciberespacio y fueron llenadas con mensajes en portugués. La misma suerte, corrió la página de la AIPAC (American Israel Public Affairs Committee), la cuál fue atacada el 6 de noviembre de 2000 por un personaje pro palestino llamado "doctor Nuker". La página fue desconfigurada, obligando de tal manera a la AIPAC a clausurar temporalmente su presencia en la red.

Un caso mexicano que llamó mucho la atención, se produjo cuando el grupo mexicano "X-Ploit", en 1998, logró colapsar el servidor Web de la Secretaría de Hacienda, la Comisión Nacional del Agua, el Instituto Nacional de Estadística y el Senado de México.

Este tipo de ataque, no solamente busca generar presencia en las páginas Web atacadas; sino persigue también, demostrar que los sistemas de seguridad de sus servidores son ineficientes. Situación que puede degenerarse en un ataque terrorista.

6.5. TIPOS DE ARMAMENTO INFORMATICO

6.5.1. ARMAS LOGICAS

6.5.1.1. VIRUS INFORMATICOS

Este tipo de virus, es mucho más sofisticado que un virus normal; ya que está diseñado para actuar sobre redes de sistemas informáticos.

Estos virus pueden adoptar diferentes formas al ser creados y actuar siguiendo diferentes estrategias para conseguir su objetivo; pudiendo interferir, confundir y destruir los programas junto con la información.

Este tipo de armamento utilizado por los terroristas informáticos; puede colapsar todo un sistema informático; que por lo general, controla sistemas críticos dentro de un Estado. Es decir, el flujo de energía eléctrica, distribución de agua, control de aeropuertos, y otros.

Como cualquier otro programa informático, un virus debe ser ejecutado para que realice determinada acción: es decir, el ordenador debe cargar el virus desde la memoria del ordenador y seguir sus instrucciones. Estas instrucciones se conocen como carga activa del virus, que logra trastornar o modificar archivos de datos,

presentar un determinado mensaje o provocar fallos en el sistema operativo.

Algunos virus tienen la capacidad de adherirse a programas legítimos. Esta adhesión puede producirse cuando se crea, abre o modifica el programa legítimo (ej. Word). Los virus también pueden residir en alguna parte del disco duro o flexible que cargan y ejecutan el sistema operativo cuando se arranca el ordenador, por lo que dichos virus se ejecutan automáticamente. En las redes informáticas, algunos virus se ocultan en el software que permite al usuario conectarse al sistema.

El año 2003 se caracterizó por la aparición de nuevos virus, con especies como BugBear, Sobig o MSBlast, que lograron paralizar los servicios de reserva de al menos una aerolínea, alcanzar a numerosas instituciones públicas y privadas e incluso a una central nuclear. **([72])**

Howard Schmidt, que ocupa el puesto de vicepresidente de la Oficina de Protección de Infraestructuras Críticas (Critical Infrastructure Protection Board) del presidente Bush, también se ha referido a la problemática actual que representan los virus informáticos. "Desde

[72] SEGURIDAD en la Red, Expertos prevén un 2004 lleno de virus, http://www.el-mundo.es/navegante/2003/12/26/seguridad/1072431321.html

Bugbear a Code Red", ha explicado, "…las comunicaciones en Internet están plagadas de virus que pueden provocar un caos instantáneo…se debe continuar en la lucha contra los hackers y los terroristas informáticos, además de la necesidad de que la industria y los gobiernos de todo el mundo colaboren con la adecuación de sus normas y la sanción correspondiente…". **([73])**

6.5.1.2. BOMBAS LOGICAS

Este tipo de arma informática, es en la actualidad un instrumento muy usado por los terroristas informáticos, ya que su misión es atacar a la parte lógica del ordenador.

Se entiende por bomba lógica (time bombs), a aquel software, rutinas o modificaciones de programas que producen cambios, borrados de ficheros o alteraciones del sistema en un momento posterior a aquél en el que se introducen por su creador. Es decir, que es un programa diseñado para que se ejecute en un determinado momento en el que se cumpla una condición dada, y no en el momento de la infección. Los disparadores de estos programas puede ser varios, desde las fecha y hora del sistema; o la incorporación de

[73] El terrorismo informático le sale muy caro a George Bush http://www.el-mundo.es/navegante/2002/10/16/seguridad/1034768799.html

determinado código que será el que efectúe su activación.

En numerosas ocasiones se ha oído hablar de un virus que afecta a los computadores, exactamente los viernes 13 o en cualquier fecha conmemorativa de un evento; este es el típico caso de la inserción de una bomba lógica. Otra condición para la ejecución de esta bomba puede consistir en una determinada orden, por ejemplo, cuando se solicite la ejecución de un programa determinado.

Algunas de las características principales son:

- Que el tipo de actuación es retardada;
- El creador es consciente en todo momento del posible daño que puede causar y del momento que éste se puede producir;
- Este ataque está determinado por una condición que determina el creador dentro del código;
- El código no se replica;
- Los creadores de este tipo de códigos malignos son por lo general terroristas informáticos, que adecuan su accionar a una red de ataques cronometrados.

6.5.1.3. CABALLOS DE TROYA

Un Caballo de Troya o Troyano es un programa que crea una puerta trasera (es decir proporciona la posibilidad de un acceso no autorizado) al equipo de cómputo de la víctima, de tal forma que le abre un puerto (o canal de comunicación) por donde se puede acceder a su sistema. Como tales, suelen encontrarse pegados a otros programas mediante diversas utilidades específicamente diseñadas para ello, y ocultando su función real mediante la apariencia de un programa que aparentemente funciona bien, como podría ser un simple salva pantallas.

El Troyano, consta de dos partes: cliente y servidor. El servidor es quien permite que el terrorista informático, ingrese de hecho a nuestra computadora, y que tenga incluso la posibilidad de enviar nuestra dirección IP a alguna dirección de correo electrónico, a una lista de correo, al ICQ, o a un canal de IRC. Para librarnos de ellos, lo mejor es el sentido común: No aceptar regalos a desconocidos, ni ejecutables de ninguna clase. Por otro lado el cliente, es el usuario que acepta la invitación o la incorporación de dicho programa a su propio sistema informático.

6.5.2. ARMAS DE PULSO ELECTROMAGNÉTICO

Las Armas electromagnéticas son diseñadas para quemar los receptores de los equipos electrónicos adversarios y son utilizadas frecuentemente por los Ciberterroristas.

Existen los cañones HERF (High Energy Radio Frecuency) y las bombas EMP (Electromagnetic Pulse). Los primeros son emisores de alta potencia que se emplean para saturar los circuitos electrónicos. Y las Bombas EMP, provienen de explosiones atómicas o convencionales que pueden ser detonadas por Fuerzas Especiales cerca de un centro de información del enemigo.

Es decir, que este tipo de armas, provoca la destrucción física del hardware; logrando de tal manera volver inoperante al sistema informático.

Una de las características del uso de este armamento con fines terroristas; es que se realiza a distancia, usando solamente la energía electromagnética; mediante el pulso electromagnético de alta energía y de corta duración, logrando sobrecargas en los circuitos electrónicos, provocando la carbonización de los mismos.

Algo que se debe destacar, es que existen fábricas que practican el "Chipping". Que se configura en la fabricación de "chips" electrónicos vulnerables a desarrollar una determinada función no conocida por el usuario. Por ejemplo, algunos chips pueden ser

diseñados para fallar cuando reciban una señal específica o después de un determinado período de tiempo como también, que emitan una señal característica para poder ser localizados. Características que son aprovechadas por los terroristas informáticos para poder localizar a determinadas personas, sobre las que recaerán sus atentados.

6.5.3. PROGRAMAS FIRMWARE

Estos son programas que se encuentran combinados con el mismo chip; es decir, que el hardware, ya contiene un programa (software) preinstalado, el cuál no puede ser modificado. **([74])**

Esta conjunción de hardware y software inmodificable, pueden ser utilizadas por los terroristas informáticos; ya que existen determinados chips, que contienen una programación específica; que unidos a otros similares, pueden ser empleados como armas de ataque.

6.6. TIPOS DE ATAQUE

A continuación se enumeran algunos ataques Ciberterroristas, que pueden generarse:

- Ingreso a servidores militares para alterar el tipo sanguíneo de los soldados que se encuentran en plana batalla. Generando en caso de requerirse una transfusión

[74] Un ejemplo de firmware, son las tarjetas musicales navideñas, las cuales viene de fábrica con determinadas melodías.

para algún herido, la mala identificación de su grupo sanguíneo, originándole la muerte.

- Ataque a los instrumentos de navegación de los aviones, que muestran la altitud, velocidad y posición. Mostrando una información incorrecta y ocasionando el desplome de la nave o choque con otra similar.

- Infiltración en los sistemas informáticos de un hospital, logrando que los monitores se apaguen en medio de una operación.

- Ubicar determinadas bombas lógicas alrededor de una ciudad, todas transmitiendo simultáneamente patrones numéricos únicos, cada una de ellas recibiendo el patrón de la otra. Cuando una bomba cesa la frecuencia (deliberadamente, y en forma remota) detonan todas las bombas simultáneamente, logrando el colapso de determinadas vulnerabilidades de la ciudad.

- Lograr el colapso de un determinado sistema financiero mediante la discontinuidad de las transacciones, modificación en los niveles de reservas, cambiando las cuentas bancarias, borrando información, generando un caos a partir de la desconfianza en el sistema financiero del país.

- Alteración de la presión en los gasoductos ocasionando una falla de válvulas y hacer detonar un barrio o una ciudad.

6.7. ATAQUES IDENTIFICADOS

Según Mercè Molist, un especialista en Ciberterrorismo. El primer ataque de Terrorismo Informático, se suscitó en 1997, donde "el grupo Guerrillero Tamil Liberation Tigers… atacó a través de Internet a los estadounidenses, lanzando un mailbombing contra los ordenadores gubernamentales". **([75])**

En febrero de 1998. La Whale and Dolphin Conservation Society, organización británica para la preservación de los mamíferos marinos, detecta intentos de entrada en sus ordenadores provenientes de la Marina de los Estados Unidos. Objetivo Terrorista: robar un informe sobre delfines adiestrados para fines militares en el Mar Negro. **([76])**

En el mismo mes, dentro de la Operación Solar Sunrise, como la llama el Pentágono. Diversos servidores DNS de la red del Departamento de Defensa norteamericano son sistemáticamente atacados. Según el Secretario de Defensa, de ese entonces este ataque sistémico, se configuraba "…como preparación de un ataque coordinado a la Infraestructura de Información de Defensa. Que coincidió en el tiempo con los preparatorios de posibles operaciones militares contra Iraq…". **([77])**

En Mayo de 1998, el grupo "L0pht" muestra ante un comité del Senado norteamericano como es posible echar abajo los cimientos de Internet en 30 minutos, mediante un ataque sorpresivo que realizaron.

[75] Mercè Molist, "Juegos de Infoguerra", Revista "R.E.D.I. , Agosto de 1999 http://www.afcea.org.ar/publicaciones/infoguerra.htm
[76] Ibidem.
[77] Mercè Molist, Art. Cit.

Para Junio del mismo año, el grupo Masters of Downloading asegura haber robado programas militares diseñados para submarinos, satélites GPS y redes informáticas del Pentágono. El presunto terrorista informático Khalid Ibrahim, del grupo separatista indio Harkat-ul-Ansar, intenta contactar con uno de ellos por IRC y le envía un cheque de mil dólares a cambio de algunos programas. **([78])**

En Octubre, según la revista "Newsweek", la CIA ha considerado la posibilidad de entrar ilegalmente en las cuentas bancarias del líder islamista y terrorista Osama Bin Laden. Por creer que se estaría generando un ingreso de fondos mediante la intervención a sistemas informáticos de diferentes cuentas ajenas a este terrorista. **([79])**

En el mismo mes, se produce una guerra Serbia-Croacia en la Internet. El grupo serbio "Black Hand", ataca el Centro de Informática de Kosovo, a las universidades y a la versión en línea del periódico "Vjesnik". La respuesta croata es entrar en el sitio Web de la Biblioteca Serbia. "Black Hand", robando el fichero de contraseñas del "Rudjer Boskovic Institute" y se especula que consigue entrar en el proveedor de acceso a Internet más importante de Croacia. Los croatas, al final y como respuesta, entran en dos servidores serbios logrando colapsarlos. **([80])**

[78] Ibidem.
[79] www.newsweek.com
[80] www.newsweek.com

Para Noviembre del mismo año, el servicio secreto alemán intenta contratar a un estudiante, experto en la materia, para que se introduzca en los sistemas militares iraníes. Pero el joven rechaza la proposición debido a la peligrosidad de los Terroristas Informáticos. **([81])**

La historia para 1999 no es muy diferente, ya que en Enero de este año, la empresa "Connect Ireland" realiza una acusación al gobierno indonesio de estar detrás de diferentes ataques que han tumbado el principal servidor desde el que se gestionaba el dominio ".tp", correspondiente al Timor Oriental (antigua colonia portuguesa ocupada por Indonesia). La BBC News, titula a esta información: "País virtual 'nukeado' en la red". **([82])**

En Marzo, la agencia "Reuters" y un periódico londinense, "The Sunday Business", afirman que Terroristas Informáticos han tomado control de un satélite militar británico y han pedido un "rescate" por él, al gobierno. Sin embargo, el ministro de Defensa lo niega, al igual que destacados expertos en seguridad, quienes sospechan que se trate de una mala apreciación informativa.

En el mismo mes, empieza en la Internet la guerra de Kosovo, donde terroristas informáticos rusos, yugoslavos y norteamericanos, llenan páginas de graffitis (Ciberterrorismo Low Tech) a favor y en contra de Milosevic y la OTAN. **([83])**

[81] Ibidem.
[82] Ibidem.
[83] Mercè Molist, Art. cit.

La red se utiliza para poner en contacto a Ciberterroristas dentro y fuera del territorio. Nacen nuevos foros de discusión, la información de la guerra vuela por las listas, se discute los principales episodios. La red se llena de propaganda.

A finales de mayo, el presidente de los Estados Unidos de América, Bill Clinton, firma un documento por el que se decreta el cierre de un satélite, vital para algunos proveedores de Internet en Yugoslavia. Semanas después y según "Newsweek", el presidente aprueba una operación nunca antes vista: que la CIA busque y anule todas las cuentas bancarias de Milosevic en Europa. **([84])**

En Marzo del mismo año, las computadoras del gobierno norteamericano empiezan a sufrir una infinidad de ataques Ciberterroristas, que se perpetran de forma permanente hasta la actualidad. Incluso se generan ataques a máquinas militares y al sitio Web del FBI. **([85])**

Sin embargo, quizás el apagón masivo en EEUU y Canadá haga reflexionar a los gobernantes de todo el mundo, porque nadie en sus sanos cabales se cree el cuento del "apagón por un fallo técnico". La red eléctrica de EEUU y Canadá es una "malla" de seguridad, y es simplemente imposible que en una red eléctrica de estas características los disyuntores se vayan apagando uno tras otro, a menos que todos los ordenadores que los supervisan se hayan "vuelto locos".

[84] www.newsweek.com
[85] Ibidem.

Si analizamos algunos de los sucesos acaecidos en los últimos tiempos, la guerra en el ciberespacio y los ataques Ciberterroristas, no parecen ser una mera hipótesis de las muchas que se barajan en las jefaturas militares de las grandes potencias, sino que ya es un hecho. Esto parece indicar la actividad que se registra en Taiwán, país que durante el mes de febrero del año 2001 recibió 80.000 "ataques" provenientes de China continental. **([86])** Así lo señala el primer informe oficial publicado en la isla sobre la ciberactividad bélica entre ambos lados del estrecho de Taiwán.

El informe indica que en los últimos cuatro años se han registrado 250.000 ataques de Terroristas Informáticos dentro del continente. Estos ataques están dirigidos a las redes informáticas de los organismos gubernamentales, en especial de defensa, y parece que, en los últimos meses, se está llegando a incrementar tanto en el número de ataques como la magnitud de destrucción y la peligrosidad de estos.

6.8. MEDIOS PARA LA LUCHA CONTRA EL TERRORISMO INFORMATICO

6.8.1. LÓGICOS

Dentro de Sudamérica, encontramos medidas prácticas para la lucha contra el terrorismo informático, una de ellas es la utilizada por La Red Universitaria Nacional de Chile, que muestra una forma de protección, utilizando medios lógicos (programas informáticos) para

[86] www.newsweek.com.

prevenir un ataque informático, protegiendo de tal manera la información. Esta forma de protección asegura, según la Red Universitaria, la confidencialidad, disponibilidad, integridad y confiabilidad. Distinguiendo para tal objetivo 3 niveles : seguridad de los sistemas (control de password, control de claves secretas de usuarios, control de usuarios, control de acceso); seguridad en cuanto a recursos y servicios (instalación de mecanismos o dispositivos denominados firewalls o cortafuegos, cuya función principal es mantener un control del acceso a la red y los recursos); y seguridad de la información (el más importante porque es donde más participa el usuario) que tiene varios niveles como la encriptación o cifrado de mensajes, que codifica un mensaje mediante algoritmos matemáticos, de forma que sólo lo pueda descifrar quien posea la clave de descriptación. **([87])**

Una de las posibilidades en las que se trabaja es en desarrollar un software que analiza las pautas de comportamiento de los terroristas informáticos y puede así prevenir sus ataques e, incluso, la formación, financiamiento y crecimiento de organizaciones criminales. Las tarjetas de crédito y otras entidades ya usan sistemas similares para prevenir el fraude financiero. Así pueden determinar con bastante eficacia el uso que se dará a una tarjeta robada, entre otros logros. Claro que montar algo así contra el terrorismo informático es una tarea aún más

[87] REUNA, Red Universitaria Nacional de Chile http://www.reuna.cl/

difícil: en primer lugar, se requiere de gran cantidad de información estadística difícil de colectar y se necesita de masivos intercambios de información entre las empresas de telecomunicaciones, las aerolíneas, la banca y las agencias gubernamentales, entre otras. **([88])**

Por otro lado, el Departamento de Defensa de los Estados Unidos, ha desarrollado medidas de contraste a través de los sistemas Carnívoro, Echelon y Enfopol,

A continuación se hace una breve descripción de los medios lógicos que son utilizados por el gobierno de los Estados Unidos para combatir al Terrorismo Informático:

6.8.1.1. CARNÍVORO

Carnívoro es un sistema de rastreo que actúa a manera de filtro. Su denominación enmascara la sigla Dcs 1000 **([89])** y fue creado por la inteligencia estadounidense, que además, continuamente ha venido actualizándolo y produciendo nuevas y más sofisticadas versiones. **([90])** Su régimen legal y técnico se encuentra en normas muy precisas como son: las disposiciones contenidas en el título III del

[88] http://www.conectados.com.ec/paginas/printbusca.asp?idsec =34&idart=848
[89] Ibidem, A la pregunta ¿qué indica la expresión "carnívoro"?, el FBI responde que la denominación está privada de significado.
[90] Carnívoro es un software que constantemente está sometido a pruebas, las cuales han permitido establecer sus fortalezas y debilidades Una amplia relación técnica se encuentra en: www.usdoj.gov/jmd/publications/carniv_final.pdf. El software fue desarrollado por el FBI sobre una base propietaria de programas comerciales. Por ello corre sobre sistema operativo Windows 2000.

Omnibus Crime Control and Safe Streets Act de 1968 y las previstas en la Electronic Communications Privacy Act de 1986 y sus posteriores adiciones y reformas de los EEUU.

Es una herramienta de control pasivo de las comunicaciones telemáticas técnicamente comprobado **([91])** pero que al mismo tiempo ha sido ampliamente controvertido por considerar que las interceptaciones que realiza son violatorias de la privacidad y la libertad de las comunicaciones electrónicas. **([92])** Sobre el particular es necesario indicar dos puntos que aclaran su incidencia. La primera es de carácter técnico, y la segunda, de tipo legal.

La técnica revela que el Carnívoro trabaja sobre un flujo de información particularizada; Es decir, sobre un segmento de información que contenga el tráfico referido al sujeto investigado. Como filtro, el sistema permite aislar los datos según diversas claves; pero no se limita a filtrar únicamente el correo electrónico, como sí lo hacía su predecesor Omnivore, sino que está en capacidad de aislar datos de todos los protocolos

[91] La valoración técnica de Carnívoro ha sido realizada en Illinois por el Institute of Technology Research (www.iitri.com) por encargo del Departamento de Justicia de los Estados Unidos.

[92] Asociaciones pro-libertades civiles en los Estados Unidos han promovido campañas contra el uso del sistema por parte del FBI y el Gobierno estadounidense. Por ejemplo: la Electronic Privacy Information Center (www.epic.org) ha solicitado mayor información sobre cómo Carnívoro realiza las interceptaciones acogiéndose en una norma garantista llamada *Freedom of Information Act*. *Véase* este asunto en www.infoleggi.com en el artículo titulado: "La fragile liberta della rete", fechado el 15 de enero de 2002.

de la Internet comprendiendo las comunicaciones vía el canal messenger y los chat.

En lo legal se indica que las interceptaciones realizadas mediante el sistema Carnívoro requieren necesariamente autorización judicial. Además de ello, la interceptación debe proceder sólo para delitos de particular gravedad **([93])** y el sistema sólo podrá recolectar pruebas concretas (no sobre informaciones generales) para fines exclusivamente de inteligencia y sobre posibles ataques Ciberterroristas. Además se exige que la actividad investigativa se ciña estrictamente a los parámetros establecidos por la ley, so pena de la declaración de nulidad de una prueba obtenida en contra vía con esos parámetros. Las investigaciones no pueden durar más de 30 días, salvo contadas excepciones, las cuales deben estar justificadas y acompañadas de informes detallados de los progresos logrados cada siete a diez días. **([94])**

A raíz de los ataques del 11 de Septiembre, no pasaron más de 24 horas para la que la policía federal (FBI) se presentará en las

[93] Existen respecto a Carnívoro normas especiales aplicables en caso de urgencia manifiesta. Por ejemplo, para hechos como los acaecidos el 11 de septiembre en los Estados Unidos, el procedimiento cambia en cuanto a la autoridad que expide la orden y el tiempo en que ésta debe expedirse. Por ello se habla de un cierto margen de discrecionalidad por parte del FBI.
[94] www.epic.org

sedes de numerosas empresas proveedoras de servicios de conexión a Internet en ese país para solicitarles la instalación del Carnívoro. Así, pues, la nueva política antiterrorista les impone a las empresas proveedoras entregar sus registros de actividades y los correos electrónicos de personas catalogadas de sospechosas por las autoridades. **([95])**

6.8.1.2. ECHELON Y ENFOPOL

Echelon es la denominación que se le ha dado hoy al Sistema de interceptación global. Con su nombre se quiere identificar un sistema específico de interceptación satelital. Sin embargo, Echelon es más que un sistema unívoco de interceptación de comunicaciones; es, propiamente, un network (red) de recursos internacionales especializados en los diversos sectores que conforman la actividad de inteligencia. **([96])**

La interceptación efectuada por Echelon es de grandes proporciones; se cree que el número de comunicaciones que llegan al sistema es de hasta 3 millones por día. Toda la información, cualquiera sea su origen, se transforman en un

[95] www.epic.org

[96] Entre las infraestruturas y recursos con los que cuenta Echelon se encuentran antenas de transmisión satelital, por las que pasan la mayor parte de las llamadas internacionales incluidas las de celulares. Igualmente, están las redes de satélites dedicadas a la labor de inteligencia para captar señales de radio con filtros en el tráfico de voz y datos. La información más detallada sobre este tema se encuentra en: www.infoleggi.com en el artículo titulado “La fragile liberta della rete”, de 15 de enero de 2002.

formato digital que se analiza en tiempo sumamente breve por sistemas sofisticados procedentes en centros de inteligencia pertenecientes al network. La masa de información que llega a esos centros de procesamiento se filtra a través de diccionarios o de sistemas de inteligencia artificial que buscan, de acuerdo con determinados parámetros y palabras claves, información de interés de las agencias de inteligencia sea en el ámbito local como internacional. De la totalidad de las comunicaciones hechas por teléfono, fax y e-mail se aísla una mínima porción de documentos que son analizados posteriormente por agentes secretos, expertos y lingüistas.

Echelon como sistema complejo de interceptación de comunicaciones en el ámbito global se ha calificado casi perfecto. Se sabe que existe desde 1988 **([97])** al terminar la guerra fría, momento a partir del cual han circulado informaciones sobre su funcionamiento, organización y uso. Actualmente, y más aún desde el 11 de septiembre del año pasado, todo lo que se sabía de Echelon está siendo avalado por países fuertes económica y

[97] Se afirma que Echelon nace al interior de UKUSA por un pacto secreto en 1948, con el fin de colaborarse los dos países en la interceptación de las comunicaciones de radio soviéticas. Posteriormente, entran a formar parte del sistema Canadá, Nueva Zelanda y Australia. No obstante, se dice también que en estricto sentido el proyecto original Echelon nace en 1971. Véase en www.infoleggi.com, el artículo titulado. “La fragile liberta della rete”, fechado el 15 de enero de 2002.

tecnológicamente, así como por organismos como el Parlamento Europeo. Echelon está siendo administrado por los Estados Unidos conjuntamente con el Reino Unido, Canadá, Australia y Nueva Zelanda. **([98])**

6.8.2. HUMANOS

Los países que sufren de actos terroristas en ocasiones no escuchan las demandas políticas ni aun su propio interés.

El ex primer ministro de Israel tratando de encontrar una solución al terrorismo señala que: "…El terrorismo no solo se combate con medio militares, sino también con propuestas políticas…". **([99])** Y es así, el terrorismo se debe atacar desde sus orígenes y no solamente con represalias a los ataques terroristas.

Los grupos terroristas, tienden a la organización clandestina y están concientes de que pueden ser atacados, motivo por el cuál toda acción de represión en contra de ellos solo encuentra una solución temporal. Lo que a su vez justifica para ellos su manera de actuar.

Si se ataca el tema desde el origen, es decir desde su base ideológica; ya no tendrán mayor discurso para defender su fundamentación. Entonces los terroristas

[98] Actualmente son cinco las agencias de inteligencia que promuven y gestionan el Echelon, a saber: National Security Agency EE.UU. (www.nsa.gov); Government Code and Cipher School (www.gchg.gov.uk) en Reino Unido; Commmunications Security Establishmen (www.cse.dnd.ca) en Canada; Defence Signals Directorate (www.dsd.gov.au) en Australia y Government Communications Security Bureau (www.gcsb.govt.nz), en Nueva Zelanda.
[99] CHEREM, Silvia, "Entrevista a simón Peres", Reforma, México, 13 de enero de 2003, Pág. 30

informáticos, podrán ser procesados jurídicamente sin que exista de por medio una connotación política.

Para combatir el Terrorismo Informático, el Estado debe utilizar la política y la diplomacia y por ningún motivo la acción militar; ya que los políticos y los diplomáticos tienen como arma fundamental a la gestión social y a la negociación.

CAPITULO VII

ANÁLISIS JURIDICO DEL TERRORISMO INFORMÁTICO

7.1. UBICACIÓN JURÍDICA

7.1.1. DENTRO DEL DERECHO

Desde el punto de vista del Derecho Penal, el Terrorismo se manifiesta mediante la ejecución repetida de delitos, por los cuales se crea un estado de alarma y de temor en la población o en determinados grupos sociales o políticos. Situación por la que la sociedad debe defenderse y es entonces donde el Estado crea las figuras penales que reprimen esta clase de hechos.

Para poder ubicar el delito de terrorismo dentro de una clasificación general, se debe distinguir, tal cual lo señala la Enciclopedia Omeba; "…la ilicitud del fin que se propone el agente…". **([100])** De tal forma es que los delitos se clasifican en comunes y políticos.

Dentro de los delitos políticos, encontramos una segunda clasificación en: a) Delitos Políticos *Sensu stricto*; b) Delitos anarquistas; c) Delitos sociales y d) Delitos Terroristas.

De tal forma es que estudiosos dentro de la ciencia penal se han preocupado con respecto al tema. Por lo que debemos mencionar a Ferri, quién hace una distinción sobre la criminalidad; encontrando a la criminalidad común y la criminalidad política; definiendo a esta última como "criminalidad que bajo una u otra forma, procura apresurar las fases futuras del Estado o de la organización de la sociedad, de un modo más o menos ilusorio". **([101])**

El terrorismo informático y el terrorismo en general, es un delito que sólo se comete por acción, no por omisión; por lo que no hay un Terrorismo Informático culposo, sino meramente doloso.

7.1.2. DENTRO DEL DERECHO INFORMATICO

[100] ENCICLOPEDIA ELECTRÓNICA JURÍDICA OMEBA, Tomo XIX Derecho Penal, Sección Delitos Pág. 126, Sub directorio Pág. 50.
[101] FERRI, Sociología criminale – Ed. 1905, Págs. 370 a la 371.

Esta es una de las falencias del Derecho Informático, ya que dentro de la variada clasificación que existe con respecto a los delitos informáticos, no se establece como tal al Terrorismo Informático; sin embargo, e inclusive en la clasificación que la Organización de las Naciones Unidas hace con respecto al Delito informático, asemeja la figura de terrorismo como al SABOTAJE INFORMATICO, que se configura en el acto de borrar, suprimir o modificar sin autorización funciones o datos de computadora con intención de obstaculizar el funcionamiento normal del sistema. Estableciendo que las técnicas que permiten cometer sabotajes informáticos son el uso de virus, caballos de troya y otros descritos en el capítulo V de la presente Tesis. Pero en ninguna parte menciona la característica principal del terrorismo, que es la de desestabilizar el orden constitucional de un Estado.

7.2. LEGISLACIÓN BOLIVIANA

No es la amenaza potencial de la computadora sobre el individuo lo que provoca desvelo, sino la utilización real por el hombre de los sistemas de información con fines de espionaje; no son los grandes sistemas de información los que afectan la vida privada, sino la manipulación o el consentimiento de ello por parte de individuos poco conscientes e irresponsables de los datos que dichos sistemas contienen.

La humanidad no esta frente al peligro de la informática, sino frente a la posibilidad real de que individuos o grupos sin

escrúpulos, con aspiraciones de obtener el poder que la información puede conferirles, la utilicen para satisfacer sus propios intereses, a expensas de las libertades individuales y en detrimento de las personas. Asimismo, la amenaza futura será directamente proporcional a los adelantos de las tecnologías informáticas.

La protección de los sistemas informáticos puede abordarse tanto desde una perspectiva penal como de una perspectiva civil o comercial, e incluso de derecho administrativo. Estas distintas medidas de protección no tienen porque ser excluyentes unas de otras, sino que, por el contrario, éstas deben estar estrechamente vinculadas. Por eso, dadas las características de esta problemática, sólo a través de una protección global, desde los distintos sectores del ordenamiento jurídico, es posible alcanzar una cierta eficacia en la defensa de los ataques a los sistemas informáticos.

La utilización de los medios informáticos, al ser destinados al servicio de la sociedad, requieren de una inminente regulación jurídica con respecto a su utilización.

Los sistemas de computadoras ofrecen oportunidades nuevas y sumamente complicadas de infringir la ley, y han creado la posibilidad de cometer delitos de tipo tradicional en formas no tradicionales.

La aparición de nuevas formas de delincuencia en nuestro país tendientes a mantener a la sociedad en un constante sobresalto, debido a su complejidad, requieren la inmediata intervención de los órganos del Estado encargados de la

prevención y la represión de los delitos, pero dichos órganos se encuentran en la imposibilidad de actuar en tanto no existan en el derecho positivo las normas que lo establezcan.

Se debe fortalecer y ampliar el marco legal junto con los mecanismos institucionales que permitan prevenir y combatir al Terrorismo Informático. Es necesario contar con una adecuada capacidad de defensa.

Dentro de los Delitos contra la Tranquilidad Pública del Código Penal, encontramos la tipificación del delito de terrorismo, la cuál establece:

> ***Artículo 133 (TERRORISMO).-*** *"El que formare parte, actuare al servicio o colabore con una organización armada destinada a cometer delitos contra la seguridad común, la vida, la integridad corporal, la libertad de locomoción o la propiedad, con la finalidad de subvertir el orden constitucional o mantener en estado de zozobra, alarma o pánico colectivo a la población o a un sector de ella, será sancionado con presidio de quince a veinte años, sin perjuicio de la pena que le corresponda si se cometieren tales delitos".* **([102])**

En este tipo penal, se observa la distinción que se hace en cuanto a "organización armada". Si bien se entiende por "organización" a toda asociación de personas regulada por un conjunto de normas en función de determinados fines. Es preciso definir, que se entiende por "armada"; situación que

[102] Código Penal, Art. 133.

permite señalar que debido a esta palabra, el Terrorismo Informático no encuentra tipificación en nuestro ordenamiento jurídico; y si se pensaría iniciar demandar a un individuo por Terrorismo Informático, nuestra acción quedaría en la nada, porque el este tipo de terrorista utiliza a los medios informáticos (computadora e Internet) para cometer sus atentados. Y obviamente la computadora en términos generales no es considerada un arma, pero dentro del campo de delincuencia informática, sí lo es. Justamente por ello, es que la presente Tesis, pretende concienciar a quién la lee, sobre las inobservancias y vacíos legales que nuestra legislación presenta.

7.2.1. EN EL FINANCIAMIENTO

El financiamiento del Terrorismo Informático, no esta legislado dentro de nuestro país; es más, como ya se sabe, ni siquiera el Terrorismo como tal se encuentra normado; sin embargo, a raíz del descubrimiento de financiamiento a terroristas, es que se podría aplicar el Artículo 185 bis del Código Penal, modificado por la Ley 1768 de 11 de marzo de 1997, que señala.

> ***Artículo 185 bis.- (LEGITIMACION DE GANANCIAS).***- *"El que adquiera, convierta o transfiera bienes, recursos o derechos, que procedan de delitos vinculados al trafico de sustancias controladas, de delitos cometidos por funcionarios públicos en el ejercicio de sus*

funciones o de delitos cometidos por organizaciones criminales, con la finalidad de ocultar o encubrir su naturaleza, origen, ubicación, destino, movimiento o propiedad verdadera, será sancionado con presidio de uno a seis años y con multa de cien a quinientos días.

Este tipo penal se aplicara a las conductas descritas previamente, aunque los delitos de los cuales proceden las ganancias hayan sido cometidos total o parcialmente en otro país, siempre que esos hechos sean considerados delictivos en ambos países". **([103])**

Además, firmo el "Convenio Internacional para la represión de la financiación del terrorismo", aprobado por la asamblea General de las Naciones Unidas el 9 de Diciembre de 1999, y lo promulgó como Ley Nro. 2279 de 27 de noviembre de 2001.

7.2.2. EN LA ORGANIZACION

Si bien la organización terrorista, es una agrupación estructurada y permanente; últimamente, se ha visto la figura de que muchos de los terroristas informáticos, han ejecutado determinado acto terrorista (normalmente de low tech), habiéndose conocido coyunturalmente en la Internet; es decir que unificaron conocimientos, estrictamente de forma temporal. De tal manera es que se debe señalar de acuerdo a las

[103] Código Penal, Art.185 bis.

características mencionadas al tipo penal descrito en el Art. 132 del código sustantivo penal.

> ***Artículo 132.- (ASOCIACION DELICTUOSA).-*** *"El que formare parte de una asociación de cuatro a más personas, destinada a cometer delitos, será sancionado con reclusión de seis meses a dos años o prestación de trabajo de un mes a un año.*
> *Igual pena se aplicará a los que formaren parte de bandas juveniles con objeto de provocar desórdenes, ultrajes injurias o cualquier otro delito".* **([104])**

Sin embargo, aunque la figura anterior puede ser aplicada a un grupo específico de terroristas eventuales; la mayoría de los grupos terroristas, conforman toda una estructura que opera de forma permanente en pro de la concusión de sus ideales. Donde existe un líder y una basta jerarquización de funciones. Por lo que, al no existir una norma específica al accionar terrorista, es que se debe adecuar nuestro ordenamiento al tipo penal descrito en el Art. 132 bis del Código Penal, que señala:

> ***Articulo 132 bis (ORGANIZACIÓN CRIMINAL).*** *"El que formare parte de una asociación de tres o mas personas organizada de manera permanente, bajo reglas de disciplina o control, destinadas a cometer los siguientes*

[104] Código Penal, Art.132.

delitos: Genocidio, destrucción o deterioro de bienes del Estado y la riqueza nacional, sustracción de un menor o incapaz, privación de libertad, vejaciones y torturas, secuestro, legitimación de ganancias ilícitas, fabricación o trafico ilícito de sustancias controladas, delitos ambientales previstos en leyes especiales, delitos contra la propiedad intelectual, o se aproveche de estructuras comerciales o de negocios, para cometer tales delitos, será sancionado con reclusión de uno a tres años.

Los que dirijan la organización serán sancionados con reclusión de dos a seis años.

La pena se aumentara en un tercio cuando la organización utilice a menores de edad o incapaces, para cometer los delitos a que se refiere este articulo, y cuando el miembro de la organización sea un funcionario publico encargado de prevenir, investigar o juzgar la comisión de delitos". **([105])**

7.2.3. POR LOS TIPOS DE ATENTADO

El fin del Terrorismo en todas sus formas, es desestabilizar el orden constitucional de un Estado; por lo que en ocasiones, concentra su atención en la eliminación del líder nacional, para poder encontrar una vía libre de ingreso al poder. De tal forma, es que se debe encontrar un asidero legal que sancione cualquier

[105] Código Penal, Art.132 bis.

violación a las diferentes prerrogativas, que tiene un mandatario a raíz de su envestidura.

Nuestro Código Penal, en su Capitulo IV "Delitos contra el Derecho Internacional" en referencia a lo mencionado contempla:

> ***Articulo 136 (VIOLACION DE INMUNIDADES).*** *"El que violare las inmunidades del Jefe de un Estado o del representante de una potencia extranjera o de quien se hallare amparado por inmunidades diplomáticas, incurrirá en privación de libertad de seis meses a dos años.*
> *En la misma pena incurrirá el que les ofendiere en su dignidad o decoro, mientras se encontrare en territorio boliviano".* **([106])**

Por otro lado el gobierno boliviano, promulga como Ley Nro. 2289 de 5 diciembre de 2001 la "Convención sobre la prevención y castigo de delitos contra las personas Internacionalmente protegidas", inclusive los agentes Diplomáticos aprobada por la Asamblea General de las Naciones Unidas el 14 de Diciembre de 1973.

En cuanto a los atentados terroristas perpetrados a aeronaves y navíos, debemos encontrar respaldo en nuestro Código Penal, el cuál establece con la tipificación de piratería lo siguiente:

[106] Código Penal, Art. 136.

> ***Articulo 139 (PIRATERIA).-*** *"El que se apoderare, desviare de su ruta establecida o destruyera navíos o aeronaves, capture, matare, lesionare a sus tripulantes o pasajeros o cometiere algún acto de depredación, será sancionado con privación de libertad de dos a ocho años. Con la misma pena será sancionado el que desde el territorio de la República a sabiendas, traficare con piratas o les suministre auxilio".* **([107])**

Además el mismo cuerpo legal señala que:

> ***Artículo 213 (ATENTADO CONTRA LA SEGURIDAD DE LOS MEDIOS DE TRANSPORTE).-*** *"El que por cualquier modo impidiere, perturbare o pusiere en peligro la seguridad o la regularidad de los transportes públicos, por tierra, aire o agua, será sancionado con reclusión de dos a ocho años".* **([108])**

Por Ley de la República Nº 2290 de 5 diciembre de 2001, el Estado boliviano, acepta al "Protocolo para la represión de actos ilícitos de violencia en los aeropuertos que prestan servicios a la aviación civil internacional", (complementario del Convenio para la represión de actos ilícitos contra la seguridad de la

[107] Código Penal, Art. 139.
[108] Ibidem, Art. 213.

aviación civil Internacional). Firmado en Montreal el 24 de Febrero de 1988.

Y como Instrumento de Adhesión, promulga la Ley Nº 2286 de 5 diciembre de 2001, que establece el "Convenio para la represión de actos ilícitos contra la seguridad de la navegación marítima", aprobado en roma el 10 de Marzo de 1988.

Bolivia se adhiere mediante Decreto Supremo 15641 de 21 de Julio de 1979, al Convenio sobre las infracciones y ciertos otros actos cometidos a bordo de las aeronaves, firmado en Tokio el 14 de Septiembre de 1963. Junto a la Convención para la represión del apoderamiento ilícito de aeronaves", firmado en la Haya el 16 de Diciembre de 1970 y sancionada como Ley de la República mediante Decreto Supremo 15640 de 21 de Julio de 1978.

Y con la "Convención para la represión de actos ilícitos contra la seguridad de la aviación civil", firmado en Montreal el 23 de Septiembre de 1971, donde Bolivia se adhirió mediante Decreto Supremo 15642 de 21 de Julio de 1978.

Por otro lado la Ley Nº 2494 de Seguridad Ciudadana de fecha 5 de Agosto de 2003, establece la incorporación al Código Penal del tipo "fabricación, comercio o tenencia de sustancias explosivas, asfixiantes, etc.", la cuál de forma inextensa señala:

Artículo 211 (FABRICACIÓN, COMERCIO O TENENCIA DE SUSTANCIAS EXPLOSIVAS, ASFIXIANTES, ETC.).- *"El que con el fin de crear un peligro común para la vida, la integridad corporal o bienes ajenos, fabricare, suministrare, adquiriere, sustrajere o tuviere bombas, materias explosivas inflamables, asfixiantes o tóxicas, así como instrumentos y materiales destinados a su composición o elaboración, será sancionado con privación de libertad de dos a seis años".* **([109])**

Dentro de nuestra legislación encontramos además, al Convenio para la represión de actos ilícitos contra la seguridad de la navegación marítima, aprobado en roma el 10 de Marzo de 1988 y Promulgada como Ley de la República Nº 2287 de 5 diciembre de 2001.

7.2.4. RATIFICACIÓN Y ADHESIÓN A CONVENIOS Y PROTOCOLOS INTERNACIONALES REALIZADOS POR BOLIVIA

El gobierno de Bolivia procedió a la ratificación o Adhesión de diez instrumentos internacionales de mayor importancia, relativos al terrorismo internacional, los cuales fueron promulgados como leyes de la República en fechas 27 de Noviembre y 5 de

[109] Ley de Seguridad Ciudadana, Art. 211.

diciembre de 2001, los cuales se enumeran a continuación:

INSTRUMENTO	PROMULGACION
Convención de la Organización de los Estados Americanos (OEA) para la prevención y represión de los actos terrorismo encuadrados como delitos contra las personas y actos conexos de extorsión de alcance Internacional, de 2 de Febrero de 1971	Promulgada como Ley de la República Nro. 2284 de 5 diciembre de 2001.
Convención sobre la prevención y castigo de delitos contra las personas Internacionalmente protegidas, inclusive los agentes Diplomáticos aprobada por la Asamblea General de las Naciones Unidas el 14 de Diciembre de 1973.	Promulgada como Ley de la República Nro. 2289 de 5 diciembre de 2001.
Convenio Internacional contra	

la toma de Rehenes", aprobada por la Asamblea General de las Naciones Unidas el 17 de Diciembre de 1979.	Promulgada como Ley de la República Nro. 2280 de 27 Noviembre de 2001.
Convención sobre la protección física de los materiales nucleares" firmada en Viena el 3 de Marzo de 1980.	Promulgada como Ley de la República Nro. 2288 de 5 diciembre de 2001.
Convenio sobre la marcación de Explosivos plásticos para los fines de detección", firmado en Montreal el 1 de Marzo de 1991.	Promulgada como Ley de la República Nro. 2285 de 5 diciembre de 2001.
Convenio internacional para la represión de los atentados terroristas cometidos con bombas", aprobada por la Asamblea General de las Naciones Unidas de 15 de	Promulgada como Ley de la República Nro. 2287 de 5 diciembre de 2001.

Diciembre de 1997.	
Convenio sobre las infracciones y ciertos otros actos cometidos a bordo de las aeronaves, firmado en Tokio el 14 de Septiembre de 1963.	Bolivia se adhirió mediante Decreto Supremo 15641 de 21 de Julio de 1979.
Convención para la represión del apoderamiento ilícito de aeronaves", firmado en la Haya el 16 de Diciembre de 1970	Bolivia se adhirió mediante Decreto Supremo 15640 de 21 de Julio de 1978.
Convención para la represión de actos ilícitos contra la seguridad de la aviación civil", firmado en Montreal el 23 de Septiembre de 1971.	Bolivia se adhirió mediante Decreto Supremo 15642 de 21 de Julio de 1978.
Protocolo para la represión de	

actos ilícitos de violencia en los aeropuertos que prestan servicios a la aviación civil internacional", (complementario del Convenio para la represión de actos ilícitos contra la seguridad de la aviación civil Internacional). Firmado en Montreal el 24 de Febrero de 1988.	Promulgada como Ley de la República Nro. 2290 de 5 diciembre de 2001.
Convenio para la represión de actos ilícitos contra la seguridad de la navegación marítima", aprobado en roma el 10 de Marzo de 1988.	Promulgada como Ley de la República Nro. 2286 de 5 diciembre de 2001
Protocolo para la represión de actos ilícitos contra la seguridad de las plataformas fijas emplazadas en la plataforma continental", aprobado en Roma el 10 de Marzo de 1988.	Promulgada como Ley de la República Nro. 2291 de 5 diciembre de 2001.
Convenio Internacional para la	Promulgada como Ley

represión de la financiación del terrorismo ", aprobado por la asamblea General de las Naciones Unidas el 9 de Diciembre de 1999.	de la República Nro. 2279 de 27 de noviembre de 2001

7.3. DERECHO COMPARADO

7.3.1. EE.UU.

La "Commission on Critical Infrastructure Protection" del gobierno Estadounidense, Afirmó que las redes de comunicaciones del país son cada vez mas vulnerables a sufrir un ataque terrorista a través de las computadoras, y reclama al gobierno que fije una nueva directiva dentro del National Security Council para tomar precauciones contra estos ataques, y juntar e intercambiar información entre el gobierno y el sector privado. **([110])**

Sin embargo, el gobierno de George Bush ya desde hace un par de años, le ha declarado la guerra al terrorismo informático, por lo que tomando acciones inmediatas ante lo sucedido con los atentados terroristas perpetrados a ese país, ha designado a un máximo responsable de la seguridad electrónica en los

[110] http://iblnews.com/news/print.php3?id=21931

Estados Unidos. Mención recaída en Richard Clarke. **([111])**

Clarke coordinará los esfuerzos para garantizar la seguridad de las comunicaciones, la información y los sistemas, incluidos los aspectos financieros y bancarios, los transportes, la energía, el agua, la salud y los sistemas de alerta por emergencia en los medios de comunicación.

Por otro lado EEUU crea equipo especial para combatir al Ciberterrorismo, decisión tomada por el presidente, George W. Bush, con el fin de prevenir el terrorismo cibernético, en especial para proteger las redes de información del gobierno y el sector privado.

La preocupación por el Ciberterrorismo ha aumentado tras los ataques del 11 de septiembre con aviones comerciales secuestrados en Nueva York y Washington, que han forzado al gobierno de Estados Unidos a buscar formas de protección contra una variedad de posibles ataques.

En un decreto de 10 páginas, Bush dijo que se propone evitar interrupciones de sistemas claves de información y "…en consecuencia ayudar a proteger al pueblo, la economía, servicios humanos y gubernamentales esenciales y la seguridad nacional de Estados Unidos…la protección de estos sistemas es esencial para los sectores de telecomunicaciones,

[111] http://iblnews.com/news/print.php3?id=21931

energía, servicios financieros, manufactura, agua, transporte, cuidado de la salud y servicios de emergencia". (**112**)

Bush ordenó que la oficina de administración y presupuesto de la Casa Blanca desarrolle políticas gubernamentales para asegurar la información en los sistemas, excepto los del Pentágono y las agencias de inteligencia, que están a cargo del secretario de Defensa y el director de la CIA.

El gobierno estadounidense, ha destinado para la gestión 2003 en la lucha contra el Ciberterrorismo, 2,3 billones de dólares, distribuidos entre el orden en la frontera electrónica, el Departamento de Justicia y el FBI. **(113)**

Además, 157,6 millones para actualizar sus sistemas informáticos y 21 para su programa de respuesta a Ciberataques. Destacan, en la partida, 32 millones para recolección de inteligencia, 10,9 para monitorización y 11,3 para un "…Sistema de Gestión de Datos de Vigilancia Electrónica…". **(114)**

Algo que se debe destacar es que el gobierno americano, ha destinado también un presupuesto especial para promover la "Ley para la investigación y educación en ciberseguridad", la que incorpora por su

112 http://iblnews.com/news/print.php3?id=21931
113 Ibidem.
114 http://www.whitehouse.gov/omb/budget/fy2003/budget.html - 06/02/02

parte, que los profesores se tomen periodos sabáticos para trabajar con el gobierno. **([115])**

7.3.2. ESPAÑA

El gobierno español, ha tomado conciencia del peligro que representa el Ciberterrorismo. Situación que ha despertado el interés de conocidos especialistas en el tema como Mercè Molist y Consuelo Ramón Chornet quién afirma que "es evidente que hasta hoy ninguna de las definiciones aportadas sobre el terrorismo ha resultado verdaderamente satisfactoria, y no abarcan la complejidad del fenómeno". **([116])** Es por eso que hasta ahora no se ha podido establecer con precisión cuál es el origen, medios, sujetos activos, motivos, finalidades y trascendencia real del terrorismo.

Sin embargo, España el 27 de junio de 2002, el Congreso de los Diputados españoles aprobó la LSSICE o "Ley de Internet". Un texto destinado a combatir la cibercriminalidad y el terrorismo informático.

Esta ley, minuciosamente elaborada por el Ministerio de Ciencia y Tecnología, incluye artículos liberticidas, a los ojos de los usuarios de una Red sometida a un mínimo de vigilancia. En efecto, obliga a los proveedores de acceso a Internet a conservar los datos de las conexiones, y del tráfico de sus clientes,

[115] http://www.whitehouse.gov/omb/budget/fy2003/budget.html - 06/02/02
[116] GARCIA Ramírez Sergio, en "Consideraciones sobre el terrorismo, cita a Consuelo Ramón Chornet, Pág.8.

durante por lo menos un año. Pero, gracias a la introducción de una enmienda de la oposición, esos datos no serán utilizados por los servicios de policía, o de información, más que con el aval de un magistrado. **([117])**

Los detractores del proyecto se sienten más decepcionados aún porque esperaban que su impacto se complementase tras el examen de los parlamentarios. El resultado final ha sido peor que el texto inicial. Especialmente en el caso del almacenamiento de los datos de las conexiones, por los proveedores de acceso. Así como en las modalidades prácticas de esta retención generalizada, que no se han precisado, lo que hace temer que se produzcan derivas. Por otra parte, queda por saber cuál es la autoridad administrativa que tendrá la posibilidad de cerrar los sitios que "atenten contra una serie de valores". Y todo ello, sin atentar contra la libertad de expresión. Una libertad reconocida y defendida por la Constitución española, cuyo artículo 20 protege particularmente el derecho "…a comunicar o recibir libremente una información verídica, por cualquier medio de comunicación…". **([118])**

7.3.3. GRAN BRETAÑA

La "Anti-Terrorism, Crime and Security Act", ley británica antiterrorista, aprobada a mediados de

[117] GARCIA Ramírez Sergio, Ob. Cit., pág. 9.
[118] Constitución Española

diciembre de 2001, fija en un año, por lo menos, la conservación de los datos de conexiones de los internautas, por parte de los proveedores de acceso. Donde se podrá "…tener derecho a mirar las transacciones financieras en línea, y a controlar los e-mails privados…". **([119])**

En virtud de la nueva ley, en muchos de los casos la policía no necesita una autorización previa del juez, para actuar. Para hacerlo, le basta con conseguir la luz verde del Ministro del Interior, o de uno de sus altos funcionarios. Una serie de medidas que provocaron una gran indignación, al otro lado del Canal. Incluso, algunos proveedores de acceso anunciaron que estaban estudiando la deslocalización de sus servidores informáticos, fuera de Gran Bretaña. **([120])**

Parecen fundados los temores de una grave irrupción de seguridad, expresados por las ONG's de Gran Bretaña. Ya que a mediados de junio de 2002, David Blunkett, Ministro del Interior, presentó un proyecto de revisión de una ley muy controvertida, aprobada en 2000: la "Regulation of Investigatory Powers Act" (RIPA). Donde plantea que las administraciones locales (impuestos, Seguridad Social, servicios municipales, etc.) puedan acceder a los datos relativos a las conexiones de los ciudadanos a la Red, y

[119] http://www.elpais.es/suple/ciberpais/despiece.html?xref=20020905elpcibenr_4&type=Tes&anchor=elpcibred&d_date=20020905&ndpc=2
[120] Ibidem.

a sus envíos y recepción de e-mails. Esta revisión programada, en principio, para junio o comienzos de julio de 2002, provocó tal oleada de indignación, tanto en la prensa como entre los grupos de defensa de las libertades civiles, que el gobierno decidió aplazar la revisión legislativa hasta el otoño. **([121])**

Elizabeth France, Comisaria de Información de Gran Bretaña (autoridad independiente que vigila que sean preservados los derechos de los ciudadanos, en materia de acceso a sus informaciones personales), declaró que los dos textos "…entran en conflicto…", y que algunas de las medidas que contienen son anticonstitucionales. Sin embargo en la actualidad se encuentran en plena vigencia. **([122])**

7.3.4. ITALIA

Para luchar contra el terrorismo informático, el gobierno italiano hizo que se aprobara, a mediados de diciembre de 2001, una ley que permite aligerar considerablemente el proceso para poner a un sospechoso en escucha y, sobre todo, que autoriza a interceptar correos electrónicos y a conservar los datos de las conexiones y las telecomunicaciones. **([123])**

Gracias a este texto, ha aumentado considerablemente el número de funcionarios de los

[121] http://www.elpais.es/suple/ciberpais/despiece.html?xref=20020905elpcibenr_4&type=Tes&anchor=elpcibred&d_date=20020905&ndpc=2
[122] Ibidem.
[123] Ibidem.

servicios de policía, y de seguridad, que pueden recurrir a esos procedimientos. En cambio, se ha rebajado el grado, o el nivel jerárquico, de los funcionarios en cuestión, ahora habilitados para llevar a cabo esas misiones. Finalmente, no pueden divulgarse los nombres de los mencionados funcionarios ni las informaciones relativas a las modalidades de esa interceptación y requisas. Quienes incurran en contravenciones se exponen a condenas de cárcel incondicional.

A finales del año 2001, se promulgó otra ley destinada a reformar los servicios de información. En virtud de ese texto, los agentes de los servicios secretos civiles (SISDE) y militares (SISMI) pueden, con total impunidad, cometer delitos en el curso de sus misiones, exceptuando matar o herir a personas. Ahora están autorizados el robo, las requisas "secretas" y las escuchas "salvajes", telefónicas y electrónicas. **([124])**

7.3.5. SINGAPUR

Singapur ha decidido plantarle cara al Ciberterrorismo. Así el Parlamento de ese país ha aprobado un proyecto de ley que permitirá a la Policía y a las agencias de seguridad realizar redadas preventivas contra posibles piratas informáticos.

[124] http://www.elpais.es/suple/ciberpais/despiece.html?xref=20020905elpcibenr_4&type=Tes&anchor=elpcibred&d_date=20020905&ndpc=2

El ministro de Interior del país asiático, **Ho Peng** Kee, ha declarado que, dado el actual clima en asuntos de seguridad en **Singapur**, "…este nuevo proyecto de ley reforzará enormemente la capacidad de nuestras agencias de seguridad para controlar amenazas informáticas, sobre todo amenazas terroristas…". **([125])**

La nueva ley permitirá realizar redadas a posibles Ciberterroristas si se cree que existe un peligro real contra la seguridad nacional.

La renovada legislación informática aplicará además multas de hasta **5.700 dólares** y tres años de prisión para aquellos Ciberterroristas que intenten penetrar redes informáticas ilegalmente. **([126])**

7.3.6. SUDAFRICA

La Asamblea Nacional Sudafricana ha aprobado la controvertida ley destinada a proteger al país contra el Ciberterrorismo.

Esta ley autoriza a la ministra de Comunicaciones, Ivy Matsepe-Casaburri, a nombrar inspectores para controlar el contenido del sistema de comunicaciones, realizar embargos y regular las bases de datos especialmente protegidas, como salud, bancarias, y otros. **([127])**

[125] http://www.plus.es/codigo/noticias/ficha_noticia.asp?id=314866
[126] Ibidem.
[127] http://delitosinformaticos.com/noticias/1023616712803.shtml

La ministra declaró ante los diputados que la intención no era controlar el comercio electrónico en Sudáfrica por los poderes indirectos que le concede la ley de Transacciones y Comunicaciones Electrónicas y asimismo, reconoció las reservas mostradas por el sector privado ante esos poderes. **([128])**

Un diputado del partido de la oposición Movimiento Democrático Unido (UDM), Salam Abram, declaró que los "…ataques podrían venir de medios electrónicos que podrían ser extremadamente devastadores…el espectro del Ciberterrorismo, el terrorismo a través de medios electrónicos, puede desestabilizar a cualquier país o nuestra situación financiera. Se trate o no de una función policial, la ley debe proporcionar una protección necesaria…". **([129])**

Es importante recordar el concepto de terrorismo que se contiene en la Convención africana, toda vez que es uno de los pocos instrumentos en el que se ha formulado una caracterización de ese delito.

De acuerdo con el artículo 1o. núm. 3 de la Convención de la Organización de la Unidad africana (hoy Unión Africana) para la Prevención y el Combate del Terrorismo:

Acto terrorista significa:

[128] http://delitosinformaticos.com/noticias/1023616712803.shtml.
[129] http://www.noticiasdot.com/publicaciones/2002/0602/1006/noticias1006/noticias1006-15.htm

a) cualquier acto que constituya una violación de las leyes penales de un Estado Parte y que pueda poner en peligro la vida, la integridad física o libertad, o causar un grave daño o la muerte de cualquier persona, de un grupo de personas o causar daños a la propiedad, pública o privada, a los recursos naturales, al medio ambiente o al patrimonio cultural, así como la planificación e intento de:

i) intimidar, atemorizar, forzar, coercionar o inducir a cualquier gobierno, cuerpo, institución, al público en general o a cualquier segmento del mismo, para hacer o abstenerse de realizar cualquier acto, o para adoptar o abandonar un determinado punto de vista o para actuar de acuerdo con ciertos principios; o
ii) interrumpir cualquier servicio público, la entrega de cualquier servicio esencial para el público o crear una emergencia pública; o
iii) crear una insurrección general en un Estado.

b) cualquier promoción, auspicio, contribución para ejecución, ayuda, incitamiento, aliento, atentado, amenaza, conspiración, organización o procuramiento de cualquier persona, con la intención de cometer cualquier acto a los que se refiere el párrafo (a), incisos (i) al (iii). **([130])**

[130] Convención de la Organización de la Unidad africana, Art. 1, num., 3.

CONCLUSIONES

El terrorismo es una de las prácticas más crueles, sangrientas e inmorales que existen. Sea cuál fuere su causa, el uso del terror para infundir miedo y zozobra en la población, no es justificado.

El uso de los nuevos medios tecnológicos, por parte de los terroristas; se ha configurado en el llamado "Terrorismo Informático", el cuál se sirve del avance informático para perpetrar sus actos.

Nuestro país, así como la mayoría de los países del mundo, no ha asumido la dimensión real del problema; desatendiendo sus sistemas de seguridad informática y de control, así como la concientización a la población en su conjunto y la creación de medios de protección a través de sus diferentes instancias.

No existe un adecuado y eficiente control de los sistemas informáticos que controlan los puntos de seguridad informática de Estado y de servicios críticos dentro del país, como lo son el control de aguas, distribución de energía eléctrica, control en gasoductos y otros.

Bolivia, tiene la obligación de analizar la perspectiva jurídica que conlleva el Terrorismo Informático; a fin de establecer todos los instrumentos legales necesarios para brindar un clima de seguridad y protección a la población e infraestructura; así como el resguardo de nuestra soberanía.

RECOMENDACIONES

A través del análisis y la perspectiva jurídica que el Terrorismo Informático conlleva, se debe concentrar esfuerzos en fortalecer uno de los pilares fundamentales dentro de la estabilidad política, económica y social del país, el cuál es precautelar la soberanía de nuestro territorio; otorgando seguridad política y jurídica con respecto al Terrorismo Informático.

Debe existir un trabajo conjunto interinstitucional, entre la Unidad de Coordinación Antiterrorista del Ministerio de la Presidencia, la Unidad de Inteligencia del Ministerio de Gobierno, la Policía Nacional, el Poder Judicial y la población civil; a fin de lograr políticas de concientización, prevención y sanción al Terrorismo Informático.

En función a las políticas adoptadas, se debe crear una ley específica, que establezca el concepto, magnitud y peligro que enmarca el Terrorismo Informático. Logrando de tal manera, llenar los vacíos legales que contiene nuestro ordenamiento jurídico vigente.

Se debe lograr el apoyo internacional en cuanto a la capacitación adecuada para el resguardo de la seguridad nacional y la estabilidad constitucional y democrática, contra atentados Ciberterroristas, suscribiendo para ello convenios internacionales con organizaciones como Amnistía Internacional y otras.

Deben realizarse cursos y seminarios, en las Instituciones mencionadas, así como a toda la población, que promuevan la

concientización sobre el peligro que representa el uso de medios informáticos con fines terroristas y la consiguiente aplicación de medidas de seguridad en sistemas informáticos de servicios críticos de control.

BIBLIOGRAFIA

LIBROS

FERRERO, Guglielmo
1972
"The Principles of Power"
Tomo I
Ed. Arno Press
New York - EEUU

GARCIA, Sergio
1982
"Consideraciones sobre el terrorismo"
Ed. Porrúa
D.F. - México

LIMA DE LA LUZ, María
1995
"Delitos Electrónicos"
Ed. Porrúa
D.F. - México

MATHIAS, Paul
1998
"La ciudad de Internet"
Biblioteca del Ciudadano
Ed. Bellarta
Barcelona - España

FERRERO, Guglielmo
1972
"The Principles of Power"
Tomo I
Ed. Arno Press
New York – EEUU

MEZGER, Edmundo
1985
"Derecho Penal – Parte General"
Sexta Edición
Editorial Cárdenas – México

PARKER, Clark
1983
"Crime By Computer"
Edición electrónica

STERLING, Bruce
1999
"The Hacker Crackdown"
Freeware literario
Traducido al castellano
por Criptópolis.

VILLAMOR, Fernando
2003
"Derecho Penal Boliviano
Parte General"
Tomo I
Editorial Popular La Paz – Bolivia

VON LISTZ, Franz
"Tratado de Derecho Penal"
Traducido por Luís Jiménez
de Asúa.
Editorial Reus. Madrid – España

SUNT ZU,
"El Arte de la Guerra"
Edición electrónica

ENCICLOPEDIAS Y DICCIONARIOS

CABANELLAS, Guillermo
1989
"Diccionario Enciclopédico
de Derecho Usual"
Tomo VIII
Editorial Heliasta.

ENCARTA **"**ENCICLOPEDIA ELECTRÓNICA"
2004 Versión electrónica
Microsoft Corporation.

NEW HACKER'S, "DICTIONARY"
2002 Traducido por Eric Raymond

OMEBA "Enciclopedia Electrónica Jurídica"
2003 Derecho Penal
Tomo XIX

RIBO, DURAN**,** Luis "Diccionario de Derecho"
1987 Editorial Bosch.
Barcelona - España

CÓDIGOS Y LEYES

CONSTITUCIÓN POLÍTICA DEL ESTADO, (Reformada por Ley Nº 2659 de 13 de Abril de 2004.

CÓDIGO PENAL BOLIVIANO, de 1834

CÓDIGO PENAL BOLIVIANO, Elevado a Ley de la República por Ley Nº 1768 de 11 de Marzo de 1977.

CÓDIGO DE PROCEDIMIENTO PENAL, Ley Nº 1970 de 25 de marzo de 1999.

LEY DE SEGURIDAD CIUDADANA, Ley Nº 2494 de 5 de Agosto de 2003

ARTÍCULOS PUBLICADOS

CHEREM, Silvia, "Entrevista a simón Peres", Reforma, México, 13 de enero de 2003, Pág. 30 A.

JOSJ, Tryangiel, "And Justice for …", 26 de Noviembre de 2001.

LEVENE, RICARDO Y CHIAVALLOTI, Delitos Informáticos, VI Congreso Iberoamericano de Derecho e Informática.

PÁGINAS WEB

http://www.ba.ucsa.edu.ar/isco/doc/Tr4.htm

BARTOLOMÉ, Mariano César, "*El terrorismo como amenaza transnacional"*. Conferencia dictada en el Primer Seminario sobre Seguridad Pública, auspiciado por el Gobierno de la Provincia de Tucumán, noviembre de 1997.

http//usinfo.state.gov/espanol/

DEPARTAMENTO DE ESTADO DE EEUU.

http://www.guiadevacunacion.com.ar/notas/nota8.html

TOXINA DEL BOTULISMO

www.nbc.med-org/anthraxinfo/Anthraxinfo3.html

BACTERIA ANTRAX

http://www.el-mundo.es/navegante/2002/10/16/ seguridad/1034768799.html

EL TERRORISMO INFORMÁTICO le sale muy caro a George Bush

http://iblnews.com/news/print.php3?id=21123

IBLNEWS / TECNOLOGÍA, Los atentados contra Estados Unidos obligan a una revisión de la seguridad.

http://www.isurf.com.ar/98-06-junio/not_terr.htm

INTERNET SURF, Revista Electrónica,

http://www.hiperactivos.com/bioterrorismo.shtml

LISTADO DE AGENTES utilizados por los bioterroristas

http://www.afcea.org.ar/publicaciones/infoguerra.htm

MERCÈ MOLIST, ciber – periodista español, "Juegos de Infoguerra", Revista "R.E.D.I. , Agosto de 1999.

http://www.reuna.cl/

REUNA, Red Universitaria Nacional de Chile

http://www.conectados.com.ec/paginas/printbusca.asp?idsec=34&idart=848

SOBRE MEDIOS LOGICOS para combatir al terrorismo informático

http://www.el-mundo.es/navegante/2003/12/26/seguridad/1072431321.html

SEGURIDAD EN LA RED, Expertos prevén un 2004 lleno de virus.

http://www.24horas.com.pe/tecnologia/1035228287.php

TERRORISMO INFORMÁTICO GOLPEA ECONOMÍA MUNDIAL.

www.computerworld.com

Variedad de Artículos

SITIOS WEB GUBERNAMENTALES DE ESTADOS UNIDOS

http://www.whitehouse.gov/homeland/index.es.html
OFICINA DE LA SEGURIDAD del Territorio Nacional

http://thomas.loc.gov/home/terrorleg.htm
CONGRESO: LEGISLACIÓN VINCULADA CON LOS ATAQUES DEL 11 DE SEPTIEMBRE.

http://www.state.gov/www/global/terrorism/index.html
DEPARTAMENTO DE ESTADO: OFICINA DEL COORDINADOR PARA EL CONTRA-TERRORISMO

http://www.treas.gov/ofac/
DEPARTAMENTO DEL TESORO: OFICINA DE CONTROL DE ACTIVOS EXTERNOS

http://www.usfa.fema.gov/nfa/tr_ertss.htm
ACADEMIA NACIONAL CONTRA EL FUEGO

http://www.fema.gov/library/terror.htm
AGENCIA FEDERAL DE MANEJO DE EMERGENCIAS

http://www.defenselink.mil/other_info/terrorism.html
DEPARTAMENTO DE DEFENSA

http://www.fbi.gov/library/terror/95report/terrusa.htm
OFICINA FEDERAL DE INVESTIGACIONES (FBI)