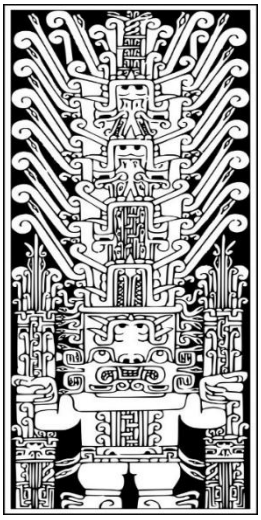
UNIVERSIDAD NACIONAL FEDERICO VILLAREAL
ESCUELA UNIVERSITARIA DE POSGRADO



TESIS

«LA FIGURA DEL CIBERTERRORISMO COMO PROPUESTA DELICTIVA PARA LA CREACIÓN DE UNA NORMA ESPECIAL EN NUESTRA LEGISLACIÓN PERUANA VIGENTE»

PRESENTADO POR:
DAVID ALONSO, SANTIVAÑEZ ANTUNEZ

Para optar el grado académico de:
MAESTRO EN DERECHO PENAL

Lima - PERÚ
2018

AGRADECIMIENTO

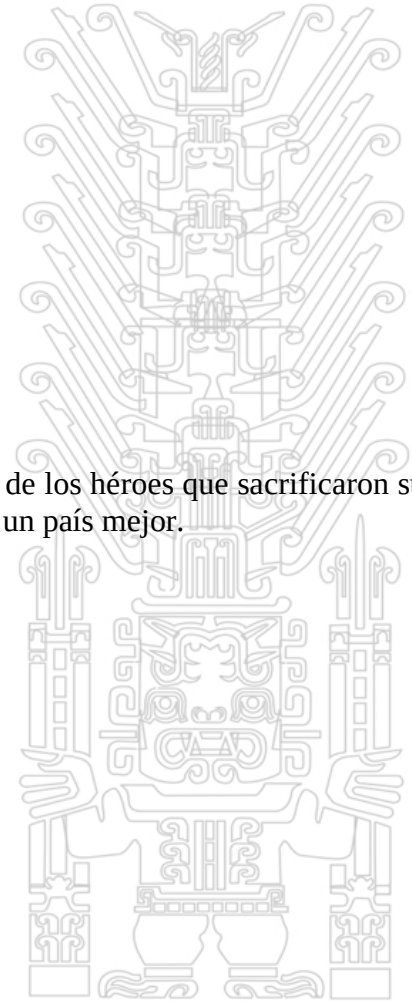
En primera instancia, agradezco a Dios por la vida y la salud, por todo aquello que brinda el mayor sentido a mi existencia.

A mi esposa Selene, la razón de mi vida y mi mayor fortaleza, la mujer que me ha impulsado a seguir en este camino de la investigación y el Derecho; a crecer y ser mejor como profesional y como persona.

A mis padres y a mi familia, quienes día a día tienen palabras de aliento para continuar en este camino de la investigación y contribuir con su contenido en el campo digital.

A mis maestros, compañeros de Maestría y mi nueva Alma Mater, que me brindaron los mejores 02 años de experiencia en el ámbito académico y que hoy, en esta tesis, se ven reflejados los esfuerzos de la educación brindada.

Finalmente, agradezco a todo aquel que lea estas páginas. Que esta investigación dé paso a muchas más, y permita que la lucha contra el ciberterrorismo y la defensa de los DD. HH. no desista.



Dedicado a todos y cada uno de los héroes que sacrificaron su vida en la lucha contra el terrorismo para hacer de este un país mejor.

INDICE

RESUMEN

El ciberterrorismo como figura delictiva y como amenaza en constante desarrollo es una de las mayores problemáticas para muchos gobiernos del mundo moderno, no solo porque esta figura emplea Internet y las TIC en su accionar cotidiano, sino por lograr la rotura de barreras tradicionales de ataque —como el campo físico— y la construcción de impacto masivo en tan corto tiempo.

Es en este mismo mundo moderno en donde la presencia jurídica a resaltado por su marcada ausencia, ya sea por el desconocimiento del campo de la seguridad cibernética, de las actividades ilícitas en el ciberespacio, la evolución de las tecnologías o el poco interés que se le da al tema. A pesar de que el Derecho solo significaría el 5% de solución del problema, es un 5% que abre puertas para un campo que se niega a seguir avanzando con la sociedad y fuerza a esta a que detenga su progreso para inadaptarse con el marco jurídico.

Es por ello por lo que surge la necesidad de poner sobre la mesa la presencia del Derecho como respuesta ante el rápido crecimiento de la criminalidad cibernética y la presencia del ciberterrorismo, figura que ya habita en la sociedad peruana y que se desenvuelve aprovechando los estándares jurídicos actuales que aún no terminan de contemplar los vacíos legales que los propios juristas han y siguen ocasionando, y más aún, por la constante negativa de trabajar de la mano con el sector técnico e impulsar el sector académico.

La tesis presentada es el resultado de más de 05 años de investigación en el campo jurídico, técnico y social, que expone la problemática de la figura del ciberterrorismo en el sector nacional e internacional, y lo que significa la ausencia del Derecho para la lucha contra esta amenaza, sin dejar de lado la exposición de propuestas y como la sociedad peruana se vería más beneficiada si el campo jurídico trabajara de la mano con el sector técnico y hacker.

Para ello, se empleó el método cualitativo realizando estudios de campo, entrevistas a reconocidas figuras en el sector de la ciberseguridad e investigación, así como recolección de datos extraídos de los principales informes emitidos por organismos internacionales y empresa privada, así como de *journals* especializados e investigaciones en el campo de la seguridad cibernética —a carencia de material bibliográfico en el campo jurídico—, con el propósito de tener datos suficientes que demuestren que el ciberterrorismo es una amenaza real, constante y sin solución —momentánea— en el Perú, y que se requiere de una respuesta inmediata para dar pie a las primeras propuestas. El resultado final es un trabajo que motiva al Derecho a regresar a su raíz de adaptación social y ocupar su lugar en esta nueva cadena evolutiva que requiere de su presencia para seguir progresando.

INTRODUCCIÓN

Hablar de una figura como el ciberterrorismo es adentrarnos en el presente de la sociedad humana y comprender que el futuro sufrió una atemporalidad y vivimos en él, aunque no lo parezca. Todo aquello que trajo consigo Internet y la tecnología nos sumerge en un mundo en donde lo límites ya no son límites, sino retos a superar o candados a romper para conocer más claramente el intelecto humano. Sin embargo, así como constructiva es destructiva nuestra conducta, y sus límites e implicancias son desconocidas.

El Estado peruano ha tenido múltiples oportunidades para debatir un tema tan delicado como este en cada una de las reuniones y mesas de trabajo en donde nuestra ciberseguridad es tema de conversación; sin embargo, nuestra principal debilidad es nuestra mayor carta de presentación y me refiero a la carencia de visión en estos últimos años. Si bien deseamos avanzar en la proyección de una mayor cultura digital, ser un Estado digital y preservar lo establecido en nuestra agenda digital, será necesario preguntarles a nuestros mayores representantes si el término digital va más allá del tema Internet o ciber, o si realmente conocen sobre el trabajo que vienen realizando.

Más que solo un trabajo legislativo, hacer frente a la figura del ciberterrorismo consiste en un trabajo que debe apoyarse también en el campo social y académico, y eso es lo que la presente tesis pretende demostrar, la necesidad de un trabajo que englobe todos esos focos y que despierte al país ante la necesidad de estar preparados para afrontar a una de las figuras que las organizaciones más importantes del mundo no solo han calificado como real, sino con el mayor foco de peligro para la humanidad.

Es deber de todos mirar hacia adelante y plantear una estrategia que permita estar preparados ante la inminente amenaza que constituye la figura del ciberterrorismo. Para ello será necesario comprender sus conceptos, la figura del ciberterrorista y saber con claridad a que nos enfrentamos. En las siguientes páginas se buscará responder cada una de las dudas que surjan con el trayecto de la investigación, para finalmente terminar con una propuesta que nos permita tener un camino por el cual cruzar, con aciertos y/o errores, pero que al fin y al cabo se transforma en una alternativa para un trabajo en equipo o para discusiones próximas en materia legislativa; porque debemos comprender que debe ser el Derecho nuestra primera barrera y respuesta ante los daños que el ciberterrorismo pueda causar y que queda escaso tiempo para reaccionar.

El Autor

CAPÍTULO I
PLANTEAMIENTO DEL PROBLEMA

1. Descripción de la realidad problemática

La figura del ciberterrorismo es una realidad internacional y considerada como una conducta de alta peligrosidad, que ya se ha presentado en el Perú a través de diversos elementos en Internet; no obstante, no existe un reconocimiento de esta figura como delito, ni una legislación vigente que permita sancionar dicha conducta, ni contamos con la tecnología para contrarrestar un ciberataque producto del ciberterrorismo.

2. Definición del problema

2.1. Problema principal

¿Debe considerarse a la figura del ciberterrorismo como una figura delictiva en el Perú?

2.2. Problema secundario

- Qué tipo de figura delictiva sería la figura del ciberterrorismo: ¿Delito contra el Estado o simplemente un ciberdelito?
- ¿El Perú cuenta con tecnología suficiente para poder combatir o resistir un ciberataque derivado de la figura del ciberterrorismo?

2.3. Formulación del problema

La figura del ciberterrorismo es una realidad internacional y considerada como una conducta de alta peligrosidad, que ya se ha presentado en el Perú a través de diversos elementos en Internet; no obstante, no existe un reconocimiento de esta figura como delito, ni una legislación vigente que permita sancionar dicha conducta, ni contamos con la tecnología para contrarrestar un ciberataque producto del ciberterrorismo.

3. Objetivo de la investigación

3.1. Objetivo general

Establecer la necesidad de que en nuestro país se tipifique como delito la figura del ciberterrorismo.

3.2. Objetivos específicos

- Analizar el tipo de figura delictiva que corresponde la figura del ciberterrorismo.
- Determinar si el país cuenta con la tecnología y elementos legales suficientes para combatir o resistir un ciberataque a causa de la figura del ciberterrorismo.

4. Justificación, importancia y limitación de la investigación

4.1. Justificación de la investigación

La principal propuesta, materia de estudio y formulación de la presente Tesis, se expresa en la necesidad de considerar como delito a la figura del ciberterrorismo en nuestro país y en nuestra legislación, ante la peligrosidad que este demuestra a nivel internacional desde hace más de diez (10) años hasta nuestro tiempo; pero, además, formular una ley especial que determine su penalización que permita establecer las sanciones que reciban los actores que cometan el futuro delito, esto debido a la importancia de la materia que regula, que afecta tanto a la seguridad nacional como a la seguridad ciudadana.

4.1.1. *Teórica*

El propósito de la presente investigación es aportar los conocimientos necesarios sobre la problemática del ciberterrorismo a nivel nacional e internacional, así como los puntos clave en los que el Derecho debe aplicar su experticia y así ser parte del armazón que nos permita estar preparados para afrontar esta amenaza, y cuyo resultado podrá sintetizarse en la elaboración de un proyecto de Ley que permita considerar al ciberterrorismo como un delito dentro de nuestra legislación.

4.1.2. *Práctica*

La presente investigación se realiza a razón de la necesidad de regular el ciberterrorismo en nuestro país ante la peligrosidad que esta representa para la sociedad y que ha quedado expuesta en los múltiples reportes presentados por organizaciones internacionales.

4.1.3. *Metodología*

Para la presente Tesis se utilizará dos métodos de trabajo:

a. **Método Inductivo:** *Parte de información recogida mediante sucesiva observación para establecer ley mediante generalización. Se basa en verdades particulares para llegar a verdad universal.*
A efectos de viabilizar este método, durante el lapso de las primeras 04 semanas de iniciado el desarrollo del trabajo se procederá a la recolección de información basada en el tema materia de investigación, la mismas que se clasificará en:
   - Material bibliográfico
   - Investigaciones académicas
   - Reportajes en prensa escrita
   - Reportajes en prensa digital
   - Conversatorios y seminarios
   - Entrevista a especialistas

b. **Método de Análisis:** *Operación intelectual que consiste en considerar por separado las partes de un todo.*
Toda aquella recolección de información será analizada y clasificada por tema y año de estudio; para, finalmente, estudiarla detalladamente y formar un conjunto de teorías que ayuden a comprender mejor la

figura del ciberterrorismo y sus peligros a nivel nacional y global, ayudando así a resolver las hipótesis de la presente Tesis.

4.1.4. ***Social***

Con la finalidad que busca la presente investigación, centrada en la tipificación de la figura del ciberterrorismo y la creación de una ley especial para aplicar las sanciones correspondientes, se crea una protección en la sociedad peruana, tanto en el campo físico y como cibersociedad, permitiendo así la protección de los principales derechos humanos en el campo tangible y virtual. De igual manera, crea un precedente a nivel internacional, toda vez que seríamos el primer país en plasmar, por medio de una legislación vigente, en sancionar la figura del ciberterrorismo, brindado así las suficientes armas legales para llegar a combatirlo.

4.2. Importancia de la investigación

La presente investigación tiene mucha importancia puesto que busca demostrar la necesidad de tipificar la figura del ciberterrorismo en nuestra legislación ante la peligrosidad que esta proyecta a nivel nacional e internacional desde hace más de diez (10) años, proponiendo la gestación de una ley especial que permita el correcto ejercicio del Derecho y la tipificación de esta figura vigente en el campo del cibercrimen.

4.3. Limitaciones de la investigación

Una de las principales limitaciones presentes durante el desarrollo de esta investigación denota en la carencia de bibliografía especializada en el sector jurídico, así como investigaciones académicas que aporten a este campo; material que sí estuvo vigente en el campo de la ciberseguridad. Así mismo, se careció de reportes de instituciones nacionales, encuestas, estadísticas o material legislativo o relacionado en este tema en el ámbito nacional.

Grandes aportes brindaron los informes especializados realizados por las principales instituciones a nivel internacional, quienes abordaban el ciberterrorismo no solo como una problemática para las tecnologías, también para el campo político, social, armamentista y, especialmente, legal.

CAPÍTULO II
MARCO TEÓRICO

1. Antecedentes de la investigación

1.1. Antecedente I – La revolución histórica de Internet y la tecnología en el campo del delito

Watchman Nee (1997) escribió que el hombre tenía tres obras importantes en su haber: (1) sus delitos; (2) sus logros; (3) sus responsabilidades. Este escrito, aunque colindando con lo cristiano de su religión, no descarta la idea de que el delito, como producto del hombre, nace con él mismo y su convivencia social. No podríamos hablar de delito su configuramos al hombre como unidad y no como conjunto. Los escritos históricos que hacen referencia a los delitos son amplios, antiguos e infinitos, solo limitados a nuestra existencia.

Cuando las primeras ideas de Internet se fueron plasmando en el universo humano, en el año 1962, nunca se pensó en una idea de delito, ni siquiera en la expansión humana y su conocimiento como lo conocemos hoy; sin embargo, la raíz del delito es intrínseca en nosotros y su expansión solo era cuestión de tiempo. Hoy por hoy, el cibercrimen es la industria delictiva más rentable del mundo[1], que augura un crecimiento de 1 billón de euros para el 2019[2] y que pone en juicio la adquisición de la información en beneficio de la seguridad nacional con la *violación* del derecho a la intimidad[3].

El delito apareció con el hombre en sociedad, y no es imposible imaginar que este evolucionará tanto como el hombre lo haga. El delito no puede vivir sin el hombre, ¿pero puede llegarse a pensar que en algún momento el hombre pueda vivir sin delito? Más allá de una respuesta banal, puede ser este la primera pista para entender como el delito cambió con el paso del tiempo y la tecnología, simplificando misiones y haciéndolas actividades más audaces en relación con nuestro tiempo.

1.1.1. *¿Cómo funciona Internet y para qué fue creado?*

1.1.1.1. *Inicios de la historia de Internet: El nuevo continente*

Normalmente escuchamos que Internet nació para intercomunicarnos, para hacernos la vida más simple, para expandir conocimientos y para llevar los límites de la existencia

[1] Cfr. **«La alta rentabilidad del cibercrimen: beneficios de hasta el 95% de la inversión en ataques DDoS»**. Publicado en la sección portal TIC del portal web del diario EUROPA PRESS, el 27 de marzo de 2017. En: http://www.europapress.es/portaltic/sector/noticia-alta-rentabilidad-cibercrimen-beneficios-95-inversion-ataques-ddos-20170327132841.html

[2] Cfr. SUCASAS FERNÁNDEZ, Ángel Luis. **«El cibercrimen, el negocio más rentable»**. Publicado en la sección ciberseguridad del portal web del diario EL PAÍS, el 16 de marzo de 2016. En: https://elpais.com/tecnologia/2016/03/16/actualidad/1458146832_730308.html

[3] **Ibid.**

humana a otros tiempos. Quizás lo mismo se dijo de espacio exterior alguna vez, y ahora se dice de la realidad virtual; pero bien es cierto que Internet llegó de manera inesperada y —quizás— sin la necesidad de tenerlo en nuestras vidas. No obstante, Internet nunca nació con el fin de **INTERCONECTAR AL MUNDO**, o al menos, eso dice su historia.

Si queremos comprender Internet como es entendido en nuestro tiempo, no será fácil entender su pasado; pero si no aceptamos ese pasado, mucho menos vamos a visualizar su futuro y por qué se habla de una nueva civilización basada en el conocimiento y la información, el bitcoin u otras *criptomonedas*, de la libertad de ser enteramente libres y del ciberdelito y el cibercrimen que no tienen fronteras y generan millones al año, con cifras que van en constante crecimiento. Entonces, es importante conocer las etapas del desarrollo de Internet hasta nuestros días.

1.1.1.1.1. Las cuatro etapas de Internet

No existe un libro o documento en sí que pueda clasificar las etapas de Internet de manera concreta. Incluso, en foros tales como el IGF se discute más sobre una industria 4.0 que un Internet 4.0; pero eso no quiere decir que este último no existe o no se esté produciendo. Luego de arduas investigaciones y participaciones dentro de las principales reuniones de Internet, me atrevo a dividir su historia y coyuntura en cuatro etapas importantes que nos permitirán entender de una manera más sencilla y dinámica el complejo mundo de la red de redes.

1.1.1.1.1.1. *Internet* 1.0

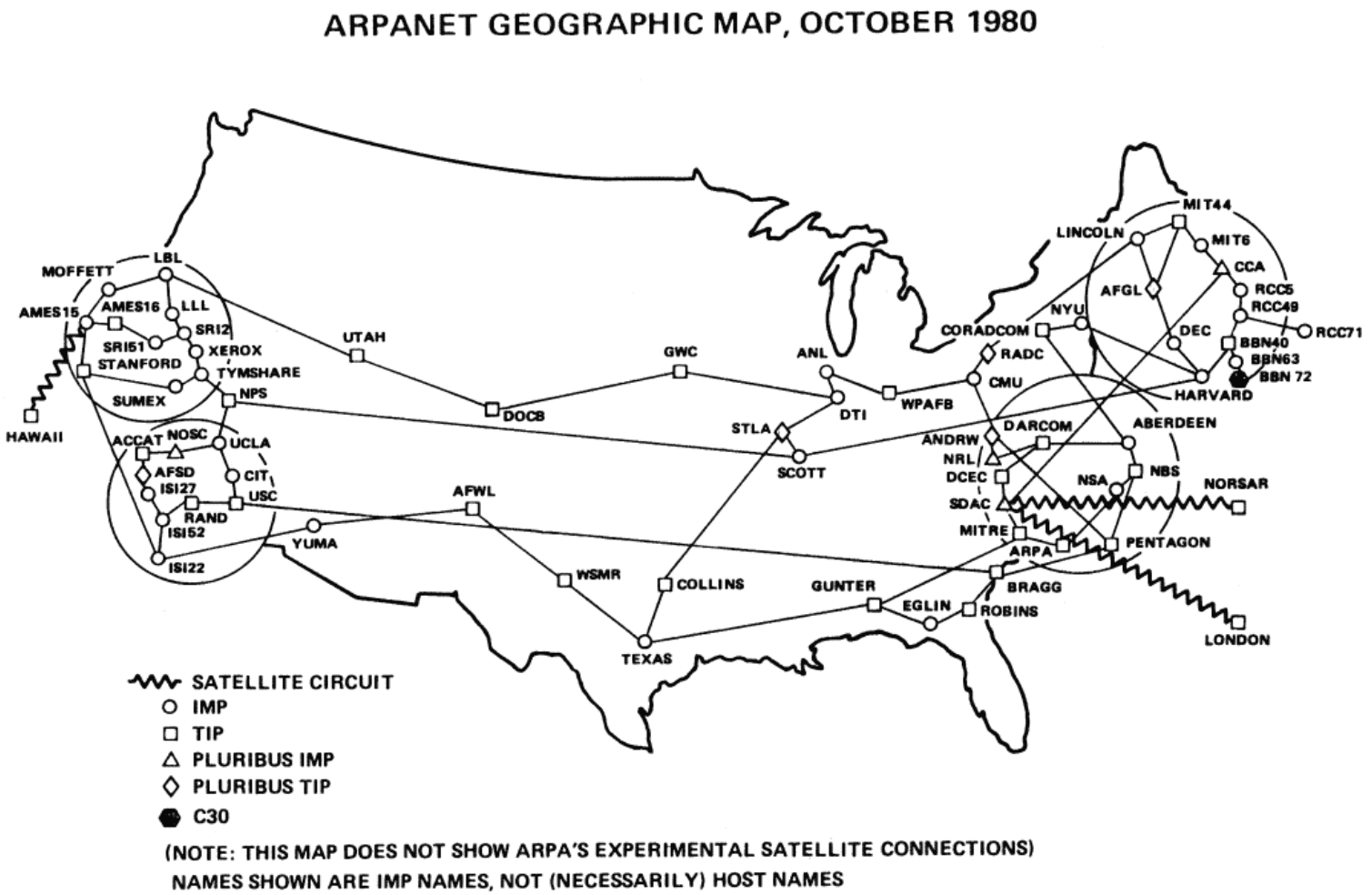
El primer paso de Internet está muy lejos de ser lo que comprendemos por Internet hoy en día. A decir verdad, dentro de este esquema podemos ubicar micro esquemas, a los cuales se les puede denominar el origen, los primeros conceptos y las ideas englobadas en la etapa intermedia, y la evolución.

Esta es quizás la etapa más enriquecedora de Internet y no por sus avances, sino por la basta historia y las bases que colocó para lo que es hoy en día; sin embargo —históricamente hablando— también es la etapa más compleja de explicar por la infinidad de hechos que marcaron un antes y un después en la formación de Internet. Es así como se analiza esta etapa de la siguiente manera.

ORIGEN DE INTERNET	
AÑO	**SUCESO**
1957-1958	Estados Unidos crea la Agencia de Proyectos de Investigación Avanzada (ARPA) dentro del Departamento de Defensa, con el fin de establecer liderazgo en ciencia y tecnología para aplicación del área militar.
Julio de 1961	Leonard Kleinrock, del MIT, publica el primer documento sobre la teoría de conmutación de paquetes.
Agosto de 1962	Primera descripción registrada de las interacciones sociales que se podían habilitar a través de la red detallado en una serie de memorandos escritos por J.C.R. Licklider, del MIT. Aparece el concepto de **«Red galáctica»**. Convence a sus sucesores e investigadores del MIT, Ivan Sutherland, Bob Taylor y Lawrence G. Roberts, de la importancia de su concepto de red.
1964	Leonard Kleinrock, del MIT, publica el primer libro sobre la teoría de conmutación de paquetes. Kleinrock convenció a Lawrence G. Roberts de la factibilidad teorética de comunicarse usando paquetes en vez de circuitos, lo que fue un gran paso en el viaje hacia las redes informáticas.
1966	Roberts ingresa en ARPA para desarrollar el concepto de redes informáticas y rápidamente creó su plan para **«ARPANET»**.
1967	Roberts publica **«ARPANET»**, un trabajo que recopila las mejores idas de los equipos del MIT, la *Rand Corporation* y el *Natinonal Physics Laboratory* (UK).
1968	Después de redefinir **«ARPANET»**, ARPA publica una solicitud de presupuesto para desarrollar uno de los componentes clave, los conmutadores de paquetes llamados IMP.
Diciembre de 1968	La solicitud de presupuesto para el proyecto IMP es ganada por Bolt, Beranek y Newman (BBN). El

	equipo liderado por Frank Heart, de la mano con Bob Kahn libraron un importante papel en el diseño arquitectónico general de lo que sería **«ARPANET»**. Por otro lado, Roberts, junto con Howard Frank y su equipo de Network Analysis Corporation, diseñaron la topología y la economía de la red. Leonard Kleinrock, junto a su equipo, preparó el sistema de medición de la red en UCLA. Se incluyen en el proyecto de **«ARPANET»** a Vint Cerf, Steve Crocker y Jon Postel. David Crocker se une más adelante, jugando un papel importante en la documentación de los protocolos del e-mail. El último fue Robert Branden, quien desarrolló en primer CNCP y luego TCP para los mainframes de IBM, quien también jugó un rol importante en la ICCB y la IAB.
1969	Se crea la red **«ARPANET»**, contando con 04 ordenadores distribuidos en distintas Universidades de EE. UU.
1970	**«ARPANET»** realiza su primera conexión a través de todo el país. Se interconectan la Universidad de California (UCLA) y la empresa Bolt Beranek and Newman, Inc. (BBN), hecho posible gracias a las instalaciones de AT&T
Diciembre de 1970	Bajo el mando de S. Crocker, Network Working Group (NWG), termina el NCP, el protocolo de host a host inicial de **«ARPANET».**
1971	**«ARPANET»**, cuenta ahora con 40 ordenadores conectados y distribuidos en distintas Universidades de EE. UU.
1972	ARPA ahora pasa a llamarse DARPA (Agencia de Proyectos de Investigación Avanzados de Defensa). Se introduce la aplicación **«hot»** inicial, el correo electrónico. Se funda **«IANA»**, encargado de la administración de

	los parámetros de protocolo, los DNS y los recursos numéricos de Internet.
Octubre 1972	Bob Kahn organiza una gran demostración de ARPANET, que tuvo mucho éxito, en la *International Computer Communication Conference* (ICCC). Fue la primera demostración pública de esta nueva tecnología de redes.
1974	Se crea **«TELENET»**, versión comercial de ARPANET.
1979	Se crea **«USENET»**, sistema abierto centrado en el e-mail (en funcionamiento). Vint Cerf establece la **«Internet Configuration Control Board»** y se convirtió en su primer presidente.
1981	Ira Fuchs y Greydon Freeman crean **«BITNET»**, red que une a las universidades americana gracias al uso de sistemas IBM. La **«NSF»** decide crear una red académica para sus computadoras. Nace la definición del protocolo **«TCP/IP»**, que permite la transmisión de datos entre computadoras; y el concepto **«INTERNET»**.
1982	Se crea **«EUENET»**, red que une Reino Unido, Escandinavia y Holanda. **«ARPANET»** adopta protocolo TCP/IP. Con ello se da nacimiento a **«INTERNET»**.



Mapa de crecimiento de ARPANET
(Fuente: Internet)

ETAPA INTERMEDIA DE INTERNET	
AÑO	**SUCESO**
1983	Se crea la **«MILNET»**, una red de comunicación militar de las Fuerzas Armadas de los Estados Unidos. Con ella se elimina el contenido militar de **«ARPANET»** y queda solo para contenido científico.
1985	Se funda el **«NSFNET»**, un programa creado y financiado por la **«NSF»**, con el fin de coordinar y promover la investigación avanzada y la educación en redes en EE. UU. Internet se establece, pero aún no es popular.
1986	Se crea **«IETF»**, organización que tiene como objetivo contribuir a la ingeniería de Internet, regulando las propuestas y los estándares de Internet (RFC).
1989	**«ARPANET»** deja de existir.
Marzo de 1989-Diciembre de 1990	Empieza el desarrollo del World Wide Web (WWW), un concepto que hace posible que la red de sitios web pueda ser buscados y mostrados con el protocolo HTTP. Finalmente, nace el término WWW.
1990	Internet empieza su camino a la popularización.

EVOLUCIÓN DE INTERNET	
AÑO	**SUCESO**
1991	Tim Berners-Lee usa un **«NeXTcube»**, computadora creada por Steve Jobs en octubre de 1988, como el primer servidor web del mundo. Se presenta al público la tecnología WWW.
1992	Internet tiene solo 50 sitios web a nivel mundial. En el mundo se encuentran conectadas aproximadamente 1 millón de computadoras. Se funda **«ISOC»,** ONG sin ánimo de lucro dedicada al desarrollo mundial de Internet. Vint Cerf se convierte en su primer presidente.

1993	Marc Andreesen del NCSA (Illinois, EE. UU.) produce **«Mosaic»**, la primera versión del navegador que permite acceder con naturalidad a la WWW, muy parecido a los navegadores actuales. Internet solo tiene 150 sitios web a nivel mundial. Empieza la etapa de crecimiento.
20 de abril de 1994	Brian Pinkerton (UW) crea y publica **«WebCrawler»**, el primer buscador web completamente de texto, que también permitía la búsqueda de imágenes, audio, vídeo, noticias, páginas amarillas y páginas blancas.
01 de junio de 1995	AOL compra **«WebCrawler»**.
1996	La guerra de navegadores: Microsoft VS Netscape. Internet Explorer y Netscape Navigator son los buscadores más utilizados para obtener información. En el mundo se encuentran conectadas aproximadamente 10 millones de computadoras.
1997	Se lanza la banda ancha de Internet. Nace la **Dot-com bubble**, un concepto que explica el éxito de la unión entre las empresas e Internet y su rápido crecimiento económico. Nace la nueva economía. Compañías tradicionales empiezan a quebrar.
01 de abril de 1997	AOL vende **«WebCrawler»** a Excite.
1998	Se funda **«CERT/CSIRT»**, centro de coordinación mundial para problemas de ciberseguridad. Solo cuando el proveedor solucionaba la vulnerabilidad de la que se le había informado, se publicaba sobre ella.
18 de septiembre de 1998	Se crea **«ICANN»**, la organización internacional y *multistakholder* responsable de asignar las direcciones del protocolo IP, de las funciones de gestión del DNS; de los identificadores de protocolo y de la

	administración del sistema de servidores raíz.
2001	Las políticas de **«CERT/CSIRT»** cambian. Ahora existe una publicación parcial, en donde se le informa al proveedor de la vulnerabilidad, disponiendo de 45 días para solucionarlo. Pasados estos, el **«CERT/CSIRT»** publicará sobre la vulnerabilidad. Explota la **Dot-com bubble** y da paso a la nueva etapa de Internet y la economía.

1.1.1.1.1.2. ***Internet* 2.0**

Esta es la parte histórica de Internet en la que empezamos a involucrarnos todos, la primera evolución después de **ARPANET** hasta su final, y en donde el WWW reina por sobre todo para las interconexiones. Aquí empieza a darse las primeras gestiones de contenido, de webs destinadas a los usuarios, a la interacción y la visualización.

Denominada así por O'Reilly Media y MediaLive International (2004), es en esta etapa en donde se presenta la mayor cantidad de componentes que conocemos el día de hoy y que son de gran explotación por arte de la comunidad digital. Markus Angermeier (2005) divide este universo de la web 2.0 de la siguiente manera:

Imagen con licencia CreativeCommons 2.0

Aquí la web se vuelve una plataforma de servicios volcada en la profunda interacción con el usuario con proyección intuitiva. Si bien mucha terminología no es de entendimiento común, los

resultados son los más comunes en la actualidad. Es por ello por lo que en esta etapa de Internet se habla de la famosa **web social**.

Ahora bien, debemos de entender que en la Internet 2.0 se habla de dos principios fundamentales íntimamente ligados: la inteligencia colectiva y la arquitectura de participación. El primero de ellos dice que, la suma del saber de cada uno de los individuos constituye un *corpus* de conocimiento, que al ser compartido puede dar lugar a una obra colectiva (ej.: www.wikipedia.org)[4]. El segundo implica una nueva forma de constituir los sitios web para permitir la participación de la gran masa de usuarios (ej.: www.mediawiki.org, web que permite a los usuarios de Wikipedia generar contenido nuevo)[5].

Arroyo Vázquez (2007) resume la filosofía de la esta era de la siguiente manera:

a) Participación y colaboración de los internautas, cuyo propósito es mayor.
b) Aumento de los canales de comunicación, que fluye en dos sentidos: de abajo arriba y de arriba abajo.
c) Mayor interacción entre los diversos agentes.
d) Compartir recursos y conocimiento de manera que otros puedan beneficiarse de ellos.
e) Democracia, en el sentido en que son los usuarios quienes ostentan el gobierno de los sitios sociales y los internautas quienes imponen las reglas de juego en estas comunidades.
f) Carácter público y apertura, ya que cualquiera puede entrar a formar parte de la comunidad de forma muy sencilla e intuitiva.
g) Obra colectiva. El resultado final es una especie de obra colectiva a la que han contribuido los mismos internautas, y de la que todos se benefician.

La era de Internet 2.0 establece los primeros cimientos para los tiempos en los que vivimos actualmente, gestores de contenido en todas las plataformas. La constante interacción con la web generó la demanda de —incluso— plataformas tradicionales de contenido a adaptarse al tiempo de

[4] Cfr. ARROYO VÁZQUEZ, Natalia (2007). **«¿Web 2.0? ¿Web social? ¿Qué es eso?»**. Revista Educación y Biblioteca, núm. 161. Madrid, España. Pp. 70
[5] **Ibid.**

Internet de ese entonces. Todavía es sorprendente que entre Internet 1.0 y 2.0 haya existido una gran valla de tiempo, a diferencia de Internet 3.0, que solo consiste en la adaptación de la tecnología, que parece acelerar más rápido que nuestra propia evolución. Al igual que la primera etapa de la historia, como sociedad, nunca imaginamos que Internet 2.0 pudiera evolucionar más y con ello forjar —a lo que es hoy— nuevos empleos y nuevos sistemas de trabajo. Finalmente había nacido un nuevo sistema de comunicación, interconexión y sociabilización que nunca fue pensado como tal, pero que se había adaptado al tiempo y al ser humano.

1.1.1.1.1.3. *Internet* 3.0

Para algunos estudiosos, esta es la etapa actual de Internet, una simple evolución —o perfección— de Internet 2.0 o Internet social. Para quien redacta, la etapa mencionada ya se encuentra superada, y nos encontramos en lo que fue Internet trabajando de la mano con la tecnología, la era que dio los primeros pasos para la *ciberdependencia*.

La era de Internet 3.0 l —término marcado aparentemente en el 2006[6]— habla de contenido libre, de evolución de redes sociales, de geolocalización, de búsquedas inteligentes y excesos de vinculación. Suena a lo que venimos viviendo con la tecnología Smart, en donde se reemplaza la búsqueda por palabras claves —típico de la era anterior— por la búsqueda por necesidades. Pero, además de esas ventajas, debemos preguntarnos que nos ofrece Internet 3.0, también llamada la web semántica[7]:

a) Búsquedas inteligentes: La web 3.0 busca crear un nuevo sistema de clasificación de páginas web estrechamente ligado a las necesidades y características de los usuarios. De esta forma, al conectarse a Internet, los usuarios pueden

[6] Existen trabajos que hablan de Internet 3.0 o Web 3.0 desde el año 2001, algunos acuñados a los gestores de la WWW, como Tim Berners-Lee (*SCIENTIFIC AMERICAN; May 2001; Volume 284, Issue 5*), quien apuntaba a un tiempo/punto exacto en que la web se transformara en un soporte para el intercambio de contenido de todo tipo, desde información hasta datos, compartidos y procesados por herramientas automatizadas y personas.

[7] CONEXIÓN ESAN (2015). **«Web 3.0: diez características que te permitirán identificarla»**. De "Sección apuntes empresariales / tecnologías". Sitio web: https://www.esan.edu.pe/apuntes-empresariales/2015/05/web-3-diez-caracteristicas-que-te-permitiran-identificarla/

disfrutar de una plataforma mucho más personalizada.

b) La evolución de las redes sociales: Crecen las comunidades sociales en la red, tanto en número como en nivel de complejidad. Aumentan también las formas de conectarse a estas redes.
c) Más rapidez: Las nuevas funcionalidades de la Web 3.0 requieren de un Internet mucho más rápido. En respuesta a esto, las principales operadoras de telecomunicaciones han implementado conexiones de banda ancha para garantizar una experiencia de uso más satisfactoria para los usuarios.
d) Conectividad a través de más dispositivos: La Web 3.0 mejora las posibilidades de los usuarios de conectarse no sólo a través de las computadoras de escritorio y laptops, sino también a través de celulares, tablets, relojes y más dispositivos.
e) Contenido libre: Los programas libres y las licencias '*CreativeCommons*' son mucho más comunes en la Web 3.0
f) Espacios tridimensionales: Los usuarios pueden acceder a nuevas formas de visualizar la web, con espacios tridimensionales. Un claro ejemplo de esto es Google® Earth.
g) Web Geoespacial: Los usuarios pueden acceder a información disponible en la red en base a su localización geográfica.
h) Facilidad en la navegación: Las nuevas tendencias de diseño buscan establecer ciertas estandarizaciones que hagan más sencilla la experiencia del usuario en la navegación, además de la creación de espacios que puedan ser modificados y personalizados por estos.
i) Computación en la nube: Con la creación de nuevos espacios de almacenamiento, no sólo de datos sino de programas, la web se convierte en un espacio ejecutable a modo de computador universal.
j) Vinculación de datos: Cada vez existen más servicios de información que son capaces de añadir datos procedentes de otras fuentes con el fin de unificar las respuestas que ofrecen a los usuarios.

1.1.1.1.1.4. *Internet* 4.0

En mi opinión, esta es la etapa actual de Internet, y lo que constituye el llamado generador de contenido. Un cambio de reglas en donde el quinto poder se instaura a razón de un teclado y a través de una pantalla, en donde la libertad de expresión se ha convertido en un libertinaje, y en donde los canales de comunicación vienen reemplazando a los tradicionales como el papel, la radio y la televisión. Entre tweets y posts, viralización y gestión de contenido, es lo que se ha dividido este nuevo camino de Internet. No es el tope, porque en treinta años (30) hemos avanzado mucho, pero no hemos llegado al final del trayecto.

El poder ha llegado de manera tan abrupta al pueblo que el control se define en las redes de comunicación masiva, llamadas para nosotros las redes sociales. Todo aquello que pisa la Red no solo permanece en ella, sino que se expande gracias a la libertad del compartir. Asimismo, la variante de la propiedad intelectual toma mayor fuerza con los *CreativeCommos* (CC) y la ideología del compartir, en donde muchos artistas renuncian a recibir regalías, pero no el reconocimiento de su nombre, con el fin de ser más conocidos y competitivos en un mundo cuya vorágine no tiene control.

También en esta etapa de Internet se produce una nueva revolución industrial conocida como la industria 4.0, la que ha establecido nuevos conceptos como Internet de las cosas (IoT), *machine to machine* (M2M), industria inteligente, manufactura 4.0, Internet de Todo (IoE) e Internet de las Cosas Industrial (Industrial IoT), entro otros variados términos que nacen día a día, impulsando así la transformación digital de la industria tradicional y la adaptación obligatoria con la sociedad. A ello también podemos agregar la aparición —y fortaleza— de la IA, el temor de los reemplazos laborales y la producción en masa con relación a las labores tradicionales —propio de cualquier revolución— y el clamor de la creación de una regulación sobre la tecnología con relación a la IA, algo *imposible* toda vez que la tecnología evoluciona cada vez más rápido, y quedaríamos constantemente desactualizados en el tiempo. En un mundo análogo como el nuestro, la relación legal con tecnología brilla por su ausencia.

La historia de Internet no termina con el hábitat 4.0 de la sociedad. Estamos en una etapa que podríamos denominar **HIPERTECNOLOGIZACIÓN** (ÁVILA-MOLINA, 2017), en donde IoT está determinando nuestro modelo de vida, desde ciertos puntos de vista. Generando nuevos conocimientos[8]. Esta empieza a ser la era de los **PROSUMIDORES**[9].

1.1.1.2. ***Gobernanza de Internet***

Como se ha podido apreciar en la historia de Internet, sus fines nunca fueron populistas, su estructura llevaba planteamiento anárquico, sin control ni desafíos, sin visión y menos sin dependencia. Decir que en la cuarta etapa puede llegar a cambiar este pensamiento, es decir que no hemos comprendido ni aprendido nada de las tres etapas antecedentes, y si de ellas hemos cometido errores, posiblemente se repitan en esta nueva, o en las venideras. La historia de Internet no concluye con una cuarta etapa. A decir verdad, es en esta en donde su nueva raíz colaborativa y humanista despierta con el nacimiento de nuevas mentas, con la aceptación de la sociedad, y con el respeto del principio que nadie gobierna Internet y que no tiene dueño; y que, a su vez, todos la gobernamos y todos tenemos dueño. Esa es una manera simple de referirnos a la gobernanza de Internet; pero ¿qué es realmente y que nos quiere decir este concepto?

La historia de la gobernanza en Internet nos remonta a los años 2003 y 2005, en donde representantes de los gobiernos, la comunidad técnica, la sociedad civil y el sector privado se reunieron en la Cumbre Mundial sobre la Sociedad de la Información (CMSI o WSIS[10]) de las Naciones Unidas, donde adoptaron la **«Agenda de Túnez para la Sociedad de la Información»**[11], y en donde se abrazaría una definición de trabajo para la gobernanza de Internet:

> «(…) *desarrollo y aplicación por los gobiernos, el sector privado y la sociedad civil, en el desempeño de sus respectivos roles, de principios, normas, reglas, procedimientos de toma de decisiones y programas comunes que dan forma a la evolución y a la utilización de Internet*» [12].

---

[8] ÁVILA-MOLINA, Oscar Noé. **ISOC Cybersecurity SIG**. 14 de septiembre de 2017. **«Webinar: ¿Esto es Ciberseguridad o Ciberdefensa? ¡No! Se trata de CiberInteligencia»**. Recuperado de https://www.youtube.com/watch?v=qWcPhbwMUKo

[9] **Ibid.**

[10] Sus siglas en inglés, World Summit on Information Society.

[11] En el año 2003 se adoptó la Declaración de Principios y el Plan de Acción de Ginebra. Para el año 2005 se adoptó el Compromiso de Túnez y la Agenda de Túnez para la Sociedad de la Información.

[12] Cfr. **TUNIS AGENDA FOR THE INFORMATION SOCIETY**. Túnez, 18 de noviembre de 2005. Documento WSIS-05/TUNIS/DOC/6(Rev. 1)-E.

Años más tardes, la UNESCO también emitiría su opinión sobre la gobernanza de Internet basado en este documento:

> «*La gobernanza en Internet es un conjunto de principios, normas, reglas, procesos de toma de decisión y actividades que, implementados y aplicados de forma coordinada por gobiernos, sector privado, sociedad civil y comunidad técnica, definen la evolución y el uso de la Red. La UNESCO reconoce el potencial de Internet para fomentar un desarrollo humano sostenible, construir unas sociedades del conocimiento inclusivas y mejorar la libre circulación de la información y las ideas en el mundo*»[13].

En ambos conceptos siempre se habla de un modelo de partes interesadas conformada por el sector privado, sociedad civil y comunidad técnica, a quienes se les ha llamado *multistakeholder* o modelos de participación múltiple, un modelo en el que cualquier actor de la comunidad o ciudadanía puede participar, conforme el párrafo 31 de la Agenda de Túnez[14]. A pesar de sus limitaciones, el modelo de múltiples partes interesadas ha demostrado ser clave para el desarrollo de Internet. Además de su creciente adopción a nivel institucional por organismos como la Organización para la Cooperación y el Desarrollo Económico (OCDE) y el Consejo de Europa, se ha convertido en un modelo cuasi oficial en las discusiones sobre una variedad de temas. Claramente, en áreas como la seguridad, la privacidad, la conectividad y los derechos humanos no existe un único punto de vista que pueda resolver problemas que por su propia naturaleza son globales y multidimensionales. En lugar de ello, el enfoque más colaborativo y de múltiples partes interesadas que se utiliza para abordar cuestiones globales relacionadas con Internet (temas de seguridad, spam, botnets, etc.) se está convirtiendo rápidamente en una mejor práctica[15]. Así mismo, debe recalcarse que la Agenda de Túnez sentó el precedente para generar el Internet Governance Forum (IGF), el foro más importante a nivel mundial y el principal espacio para debatir cuestiones relacionadas con el desarrollo de Internet, celebrado cada año[16] en una sede diferente del mundo. Si bien los participantes en el IGF contribuyen como iguales en un diálogo sobre cuestiones de políticas públicas relacionadas con Internet y su gobernanza, no tienen la autoridad para la toma de decisiones,

---

[13] ORGANIZACIÓN DE LAS NACIONES UNIDAS PARA LA EDUCACIÓN, LA CIENCIA Y LA CULTURA. **«Definición de Gobernanza en Internet»**. Recuperado del sitio web: http://es.unesco.org/themes/gobernanza-internet

[14] Cfr. **TUNIS AGENDA FOR THE INFORMATION SOCIETY**.

[15] INTERNET SOCIETY (2016). **«Informe de políticas: Gobernanza de Internet»**. Recuperado del sitio web: https://www.internetsociety.org/es/policybriefs/internetgovernance

[16] Inicialmente, el periodo de duración previsto para cada IGF era de 5 años, después de los cuales debía lanzarse una consulta formal con respecto a su continuidad, lo cual quedó establecido en el párrafo 76 de la Agenda de Túnez para la Sociedad de la Información.

pero pueden informar e inspirar a los que sí están en posición de tomarlas[17].

1.1.1.2.1. ¿Por qué gobernanza y no gobierno?

Un gobierno es un órgano superior del poder ejecutivo de un Estado o de una comunidad política, constituido por el presidente y los ministros o consejeros[18]; es decir, un gobierno se constituye bajo una nación y bajo una territorialidad. En aspectos de Internet ese es un aspecto, hasta el momento, **IMPOSIBLE** de concebir, toda vez que Internet no tiene una territorialidad definida ni un país de procedencia, no existen gobernantes ni gobiernos con autoría, pero sí con colaboración.

Hablar de gobernanza es mucho más sencillo, ya que no implica a un Estado sobre el eje y control de lo que ya se ha considerado no solo como un patrimonio de la humanidad, sino como parte del derecho humano de acceso a la información. No hay dueños para Internet, y a su vez, todos somos parte de Internet y su desarrollo. Esto podría traer meditaciones académicas, especialmente para el Derecho, ya que su escuela está acostumbrada al manejo de la territorialidad para el correcto ejercicio. Aún en este nuevo siglo, el Derecho sigue siendo una de las profesiones dependientes del lugar donde se ejerce, haciendo imposible que un canadiense o un marroquí ejerza su función como jurista al no conocer el manejo de las normas en nuestro territorio. No es lo mismo un delito en nuestra tierra como en sus países.

Sin embargo, eso es algo que con el tiempo deberá cambiar, e Internet ha puesto los primeros pasos para estas discusiones, aunque sea el mismo Derecho —o miembros de su vieja escuela— los que se oponen muchas veces a este cambio, aun conociendo la existencia de nuevas ramas en desarrollo como el Derecho espacial (**#SpaceLaw**) o el Derecho virtual (**#VirtualLaw**), legalidad que se desarrolla sobre territorios donde nuestros dominios no han sido permitidos o donde el suelo no es tangible. Incluso, algunos internacionalistas debaten la permanencia territorial del Derecho, considerando que el Derecho internacional Público será el que cambie las reglas del juego aceptando la evolución social que tiene Internet. Esto será más factible si es que el Derecho empieza a colaborar con los

[17] PÉREZ, Jorge & OLMOS, Ana (2009). **«Introducción: Gobernanza de Internet»**. Investigación: Dossier. TELOS. N°80.

[18] Definición de gobierno según la Real Academia de la Lengua Española.

multistakeholder y hacer más activa su participación en las reuniones donde se debate el futuro de la red de redes.

1.1.1.3. ***El hacktivismo y la defensa independiente***

Ingresamos a un nuevo aspecto de Internet. La coyuntura social y el desarrollo de la red de redes parecen haber ido de la mano en estos años, y ello despertó un nuevo llamado contra los sistemas opresores o contra todo aquello que pudiera ir en contra de una determinada ideología —no necesariamente de Internet—. Esto propicio el nacimiento de diversos grupos y/o movimientos, así como de organizaciones que, hoy por hoy, no solo han cambiado la historia de Internet, sino del mundo entero. Es momento de conocer un poco más de ellos.

1.1.1.3.1. **¿Qué es el hacktivismo?**
El concepto que se mal interpreta como crimen

Hablar de hacktivismo es hablar de historia, cultura, ideología, política, Internet y elementos varios. Es el acto de *hackear* o entrar a un sistema motivado por fines políticos y sociales.

El término tiene su origen en 1996, cuando 'Omega', un miembro del colectivo de *hackers* Cult of Dead Cow definió: **«Si hackear es entrar ilegalmente a una computadora, hacktivismo podría definirse como 'el uso de herramientas digitales legales o ilegales con fines políticos»**[19].

A pesar de la definición de 1996, el debate es latente en relación con sus actividades, a las que muchos no le han encontrado diferencia en comparación con actividades ciberdelictivas. Recordemos así los acontecimientos vividos en las antiguas repúblicas soviéticas de Estonia (2007) y Georgia (2008), las cuales sufrieron ciberataques que más parecían inicio de una ciberguerra que hacktivismo[20].

Según el último informe de seguridad informática de la Universitat Internacional de Valencia, el hacktivismo ya ha entrado en el podio de los mayores peligros para las grandes organizaciones. Aunque el primer puesto lo siguen ocupando los cibercriminales (con un inalcanzable 44%), el hacktivismo se alza con el segundo puesto con un 17%,

[19] ESCOBAR, Ana Cecilia (2012). **«¿Qué es el hacktivismo?»**. 2017. Del portal Daily Trend, sección *Radar*. Sitio web: http://www.dailytrend.mx/radar/101-que-es-el-hacktivismo#pageview-1

[20] PAGET, François (2012). **«¿Hacktivismo – El ciberespacio: nuevo medio de difusión?»**. McAfee®. Pp. 3.

frente al ciberterrorismo (15%), los ataques gubernamentales (12%) y la competencia directa (11%)[21].

En la práctica, el hacktivismo ha tenido momentos claves en su historia, ayudándonos a entender que quizás estuvieron presente desde la formación de Internet en sí, y que saben el porqué de su lucha, aunque muchos la consideren delictiva o poco ética.

FECHAS CLAVE Y ORÍGENES DEL HACKTIVISMO[22]	
FECHA	**COMENTARIO**
12 de septiembre, 1981	Se funda en Berlín la organización Chaos Computer Club.
1984	Se publica el libro ***Hackers: Heroes of the Computer Revolution***, de Steven Levy.
08 de enero, 1986	Se publica por primera vez el manifiesto The Hacker Manifesto, de Loyd Blankenship (alias "The Mentor").
16 de octubre, 1989	Mediante el uso del protocolo DECNET, un gusano llamado WANK (del inglés, *Worms Against Nuclear Killers*, gusanos contra los asesinos nucleares), se propaga por la red informática de la NASA en Maryland. Uno de sus objetivos era difundir un mensaje denunciando los peligros de los ensayos nucleares.
5 de noviembre, 1994 (Día de Guy Fawkes)	Los *Zippies*, un grupo de San Francisco lanza un ataque de denegación de servicio distribuida (DDoS) y una campaña de envío masivo de correo a los servidores del gobierno británico para protestar contra una ley que prohíbe los conciertos de música con un ritmo repetitivo al aire libre.
21 de diciembre, 1995	En Italia, el grupo *Strano Network* decide bloquear sitios web franceses para protestar contra los ensayos nucleares en Mururoa.

[21] NUÑEZ VILLAVEIRÁN, Luis (2017). **«Hacktivistas: la amenaza del ciberespacio»**. De PAPEL, sección *Historias*. Portal web del diario El Mundo. Sitio web: http://www.elmundo.es/papel/historias/2017/08/22/599ac51e468aeba4728b4570.html

[22] PAGET, François. **Op. cit.**

09 de febrero, 1996	John Perry Barlow publica ***A Declaration of the Independence of Cyberspace***.
30 de junio, 1997	El grupo de *hackers* portugués **UrBan Ka0s** ataca cerca de 30 sitios web del gobierno indonesio para llamar la atención sobre la opresión que sufren los habitantes de Timor.
29 de enero, 1998	En apoyo a las guerrillas zapatistas, se celebra una manifestación virtual en respuesta a una masacre cometida por fuerzas paramilitares en un pueblo de Chiapas, México.
Noviembre de 1999	**Toywar**: un acto de resistencia contra el distribuidor de juguetes eToys Inc., que había demandado a un grupo de artistas con el pretexto de que su nombre de dominio era demasiado parecido al de ellos.
03 de diciembre, 1999 4 de la tarde (GMT)	El grupo Electrohippies Collective organiza una sentada virtual, en la que todos sus seguidores deben visitar las páginas web de la Organización Mundial del Comercio para bloquear el comunicado final de la conferencia de Seattle, Washington, con el fin de impedir su difusión.
10 de junio, 2001	Para protestar contra el uso de los aviones de la compañía Lufthansa para deportar a inmigrantes sin papeles de Alemania, dos redes humanitarias alemanas organizan una protesta virtual para bloquear el sitio web de la aerolínea mediante el envío masivo de mensajes de correo electrónico.

Este mundo tiene una fina barrera que separa la legalidad de la ilegalidad. Muchas actividades delictivas han sido confundidas con hacktivismo y viceversa. Aún a pesar de que los colectivos hacktivistas luchan en defensa de las personas y sus derechos, amparados en el artículo 19 de la Declaración Universal de Derechos Humanos y el artículo 19 del Pacto Internacional de Derechos Civiles y Políticos [23], son vistos por la sociedad como elementos que dañan la estructura de Internet. La perspectiva de cambio de imagen de los hacktivistas es una tarea que no solo les corresponde

[23] Cfr. The Hacktivismo Declaration.

a ellos mismos, sino a la comunidad de Internet y los *multistakeholder* en general.

1.1.1.3.2. De Anonymous y otros grupos

De los múltiples grupos hacktivistas que existe a nivel global, Anonymous es uno de los más importante —y quizás, el más controversial—. A este colectivo se les han atribuido ataques a webs oficiales del gobierno de China, a la web de Justicia británica y al Instituto Tecnológico de Massachusetts, o el robo de un gran número de perfiles de usuario del portal SonyPictures.com en 2011. Pero quizás por el hecho que más se le conoce a nivel mundial es por declarar de forma abierta su *guerra* al Estado Islámico tras los atentados de Charlie Hebdo y Paris en noviembre de 2015. Por ejemplo, publicaron en una web el listado de unos 9.200 tuiteros, supuestamente afines y vinculados a ISIS, así como una guía para hackear el Estado Islámico, además de difundir un vídeo en el que advierten que dirigirán *numerosos ciberataques* a los yihadistas[24].

Sus orígenes se remontan al año 2003, siendo descendientes de la facción más activa "/b/", teniendo su primera aparición en los foros de imágenes públicas de la web 4chan, sin embargo, se hicieron famosos por dos hechos ajenos a foros. La primera aparición al mundo fue en el año 2006.

La segunda oportunidad se divide en dos etapas, ambas en el año 2008. En primera instancia, el 21 de enero, a través del proyecto **Chanology**[25] denunciaron las prácticas de la Iglesia de la Cienciología, las que consideraban parte de un oscurantismo que ponía en riesgo a sus miembros, los cuales terminaban aislados de sus familias. El 10 de febrero Anonymous sale a las calles cubiertos con máscaras de Guy Fawkes, héroe del comic V de Vendetta[26], para evitar ser reconocidos por los cienciólogos

[24] ROCHINA, Paula (2016). **«Hacktivismo: ¿Qué hay detrás de este movimiento activista?»**. 2017, de la revista digital de INESEM (Business School), sección *Tecnología*. Sitio web: https://revistadigital.inesem.es/informatica-y-tics/hacktivismo/

[25] El *Proyecto Chanology* (en inglés: *Project Chanology*), fue una serie de protestas que comenzaron en Internet, promovidas por Anonymous, en contra de la Iglesia de la Cienciología, en respuesta a los intentos por parte de los cienciólogos por retirar un vídeo promocional donde aparece Tom Cruise, miembro de su credo. Anonymous, el 21 de enero de 2008, lanza una vídeo respuesta denominado «*Mensaje a la cienciología*» (en inglés: *Message to Scientology*), en donde exponen que las medidas tomadas por dicha iglesia constituyen censura, por lo que buscarán expulsar a estos de Internet. El nombre también hace referencia al sitio web utilizado por este colectivo para coordinar y planificar las acciones.

[26] **«V de Vendetta»**, o **«V de Venganza»**, como fue conocido en algunos países de Latinoamérica, es una serie de comics escritos por Alan Moore e ilustrados por David Lloyd. El argumento está situado en un futuro distópico ambientada en Gran Bretaña durante un futuro cercano, a finales de la década de los 90, y tras una guerra nuclear parcial, que ocasionó la destrucción de gran parte del mundo. Según nos va

Este movimiento sirvió como ejemplo de lo que realmente defendía Anonymous, la libertad de expresión online como máxima a aplicarse en todos los países del mundo, y la lucha contra la censura por parte de los poderes y poderosos. Esto genera un debate todavía latente, pues para este colectivo hacktivista no existe diferencia entre compartir memes, momos e imágenes cualquiera, y descargar música y vídeos de manera gratuita, violando la propiedad intelectual. Todo constituye información y la información debería ser universal.

Esta no ha sido la única actividad importante ejecutada por Anonymous. A decir verdad, su historial es basto y se introduce por muchos campos de la industria digital, desde videojuegos hasta industria musical y comercial, entro otros.

FECHAS CLAVE Y ORÍGENES DE ANONYMOUS[27]	
FECHA	**COMENTARIO**
12 de julio, 2006	Gran asalto a Habbo. Primer ataque a la red social Habbo Hotel para adolescentes. En él se destaca la ausencia de personajes de raza negra.
Diciembre de 2006	Ataque al sitio web del nacionalista estadounidense Hal Turner.
Agosto de 2007	Apoyo a los monjes birmanos durante la revolución Azafrán.
05 de diciembre, 2007	Arresto del pedófilo Chris Forcand en Canadá. Parece que la policía recibió la ayuda de los miembros "cibervigilantes" de 4chan.
14 de enero, 2008	Proyecto Chanology. Carga en YouTube de un vídeo de propaganda supuestamente confidencial de la Iglesia de la Cienciología. Aunque se retiró rápidamente, la publicación del vídeo fue el trampolín para la lucha de 4chan contra los cienciólogos.
28 de marzo, 2008	Información o intoxicación. Los miembros de Anonymous han sido acusados de insertar animaciones de JavaScript y mensajes en el foro

relatando la historia, un partido fascista ostenta el poder en el Reino Unido, y es un misterioso revolucionario apodado "V", oculto tras una máscara de Guy Fawkes, conspirador católico que, según la historia, planeó **«la Conspiración de la pólvora»**, cuyo objetivo era derribar el Parlamento con explosivos situados en las bases del edificio y asesinar al Rey Jacobo I de Inglaterra, a sus familiares y al resto de la Cámara de los Lores, quién inicia una elaborada y violenta campaña con el fin de derrocar al gobierno e incitar a la población a adoptar un modelo político-social diferente.

[27] PAGET, François. **Op. cit.** Pp. 5-6

	Epilepsy Foundation con el fin de provocar migrañas y ataques en personas con epilepsia.
Junio de 2008	Los sitios de música hip-hop SOHH y AllHipHop son atacados tras publicar insultos sobre los seguidores de la red 4chan.
Enero de 2009	Un joven californiano es víctima de acoso por haber creado un sitio web para protestar contra el uso de vocabulario soez (No Cussing Club).
Abril de 2009	Operación MarbleCake. Manipulación de una encuesta de la revista Time Magazine para elegir a la persona más influyente del mundo.
Abril de 2009	Operación Baylout. Controversia alrededor de Telecom Reforms Package (un grupo de directivas de la Unión Europea contra las descargas ilegales). Ataque a la IFPI (una organización que defiende los intereses de la industria de la grabación en todo el mundo).
20 de mayo, 2009	Día YouPorn. Distribución en YouTube de vídeos aparentemente inofensivos que escondían escenas pornográficas.
Junio de 2009	Apoyo a los disidentes iraníes.
Septiembre de 2009	Operación Didgeridie (proyecto Skynet). Primera fase agresiva ("operación destructiva") para protestar contra un proyecto de ley del gobierno australiano para filtrar los datos en Internet.
Octubre de 2009	Operación CyberDyne Solutions (proyecto Skynet). Segunda fase informativa para instruir a la gente sobre cómo superar los bloqueos de Internet.
06 de enero, 2010	Día YouPorn (segunda edición) para protestar contra el cierre de la cuenta de Lukeywes1234 (conocido como el rey de /b/).
10 de febrero, 2010	Lanzamiento de la operación Titstorm. Protesta por la decisión de las autoridades australianas de prohibir la publicación de imágenes pornográficas.
Septiembre de 2010	Operación Payback. Comienza cuando una empresa india anuncia

	que ha llevado a cabo ataques de denegación de servicio (DDoS) en sitios de BitTorrent para descargar de manera gratuita vídeos y música que normalmente están protegidos por copyright. En respuesta, un gran número de sitios relacionados con la industria cinematográfica y discográfica, y de artistas sufrieron un ataque. En myce.com está disponible la cronología de esta operación.

Con un historial marcado por actividades variadas, la delgada línea de la limitación de lo legal y lo ilegal lleva a la confusión y consideración de Anonymous como grupo de crimen organizado, más no hacktivismo. Esto, a consideración personal, se debe a la ignorancia sobre el tema y a la confusión existente por parte de aquellos a quienes confiamos nuestra seguridad legal, que no han aprendido a diferenciar a un hacktivista de un delincuente.

Hoy en día Anonymous continúa activo, al igual que la confusión sobre la organización sigue latente, en parte mayoritaria, por juristas.

1.1.1.3.3. De WikiLeaks y las tendencias de la información

WikiLeaks es un servicio público *multijurisdiccional* diseñado para proteger a denunciantes, periodistas y activistas que cuentan con materiales sensibles a la comunicación al público. Desde julio de 2007, se ha trabajado en todo el mundo para obtener, publicar y defender esos materiales y, también, para combatir en el ámbito jurídico y político para los principios generales en que se basa su trabajo: la integridad del registro histórico común y los derechos de todos los pueblos a crear nueva historia[28].

Si bien la iniciativa de WikiLeaks llega a ser aplaudida como otro de los pilares de la libertad de expresión asociadas al hacktivismo, eso no ha limitado de responsabilidades a su fundador y propulsor de las libertades, Julian Assange, quien al día de hoy se encuentra prófugo de la justicia y con asilo político en Embajada de Ecuador en Reino Unido (2016) para así evadir una investigación que realiza Suecia sobre una presunta

[28] Cfr. WikiLeaks. **«About WikiLeaks»**. 2017, de WikiLeaks. Sitio web: http://wikileaks.org/

violación; y a pesar que los fiscales suecos anunciaran el abandono de los intentos de extradición el 19 de mayo de este año —no se ha determinado ni culpabilidad ni inocencia—, Assange es ahora visto como cómplice de los seguidores de Donald Trump, actual presidente de los Estados Unidos de América —país que también busca extraditarlo por liberar contenido de Estado—y de propagandistas rusos que buscaban calumniar a Hillary Clinton (ERLANGER & ANDERSON, 2017). Y aún con todo este historial en frente, Assange no deja de ser visto como héroe de la transparencia y la libertad en internet; así como un ícono de resistencia a los secretos de los gobiernos.

FECHAS CLAVE Y ORÍGENES DE WIKILEAKS[29]	
FECHA	**COMENTARIO**
Diciembre de 2006	Una nota relativa a una orden de asesinato político en Somalia.
Agosto de 2007	Un informe en el que se acusaba de corrupción al expresidente de Kenia, Daniel Arap Moi, y a su familia.
Noviembre de 2007	Manual del ejército estadounidense de 2003 en la prisión de la Bahía de Guantánamo.
Marzo de 2008	Documento interno de la Oficina de Asuntos Especiales de la Iglesia de la Cienciología.
Mayo de 2008	Documento de trabajo del Acuerdo Comercial de Lucha contra la Falsificación (ACTA, Anti-Counterfeiting Trade Agreement).
Abril de 2009	Resumen de la vista contra el pedófilo belga Marc Dutroux.
Julio de 2009	Documento interno del banco islandés Kaupthing, en el que se describían varios préstamos de mala calidad supuestamente probados por el banco unos días antes de ser nacionalizado.
Noviembre de 2009	Mensajes de correo electrónico y archivos asignados a agentes de la Climatic Research Unit (Unidad de Investigación Climática) de East Anglia (Reino Unido).
Abril de 2010	"Collateral Murder" (Asesinatos colaterales): vídeo del ejército americano en el que se ve el asesinato de dos fotógrafos de Reuters en

[29] PAGET, François. **Op. cit.** Pp. 7

	Bagdad durante un ataque aéreo el 12 de julio de 2007, grabado desde un helicóptero Apache. Apodada "Project B" por Assange, esta publicación marca el inicio de la fama mundial del sitio web.
Julio de 2010	"Afghan War Diary" (Diario de la guerra de Afganistán): 91.000 documentos militares secretos de EE. UU. sobre la guerra de Afganistán (en colaboración con The Guardian, The New York Times y Der Spiegel).
Octubre de 2010	"Iraq War Logs" (Diarios de la guerra de Irak): 391.832 documentos secretos sobre la guerra de Irak, que cubren el período que va del 1 de enero de 2004 al 31 de diciembre de 2009.
28 de octubre, 2010	"Cabelgate": WikiLeaks comienza a revelar telegramas diplomáticos estadounidenses. Anuncia que tiene más de 250.000.

No debemos confundir a WikiLeaks con Anonymous. Su estructura organizacional está diseñada para ser un puente de comunicación de información que no debió ser filtrada y como un medio que resguarda la libertad de expresión. No obstante, esto no evita que ciertos comportamientos puedan ser considerados como delito en otros países; pero ello no constituye ciberterrorismo, solo es ejecución hacktivista.

1.1.1.4. ***De los sectores público y privado en la ciberseguridad***

El último informe de ciberseguridad de la OEA y el BID (2016), afirma que algunos gobiernos de la región han comprendido el poder de Internet para su desarrollo socioeconómico y aprovechan su mayor conectividad para explotar el desarrollo de TIC, poner en marcha programas de investigación y desarrollo, y ampliar su industria. Fueron 32 países de América Latina y el Caribe los analizados bajo 49 indicadores, expresados en 05 marcos metodológicos, como política y estrategia, cultura y sociedad, educación, marcos legales y tecnologías; cuyos resultados determinaron que cuatro de cada cinco países no tienen estrategias de ciberseguridad o planes de protección de infraestructura crítica; dos de cada tres no cuentan con un centro de comando y control de seguridad cibernética; y la gran mayoría de las fiscalías carece de capacidad para perseguir los delitos cibernéticos (MORENO, 2017).

En la región no estamos preparados para afrontar las peligrosidades que ocasiona la ciberdelincuencia, y mucho menos en nuestro país, en donde se ha calculado que para fines del 2017 se registrará un aproximado de US$ 4,782M (cuatro mil setecientos ochenta y dos y 00/100 millones de dólares americanos) en pérdidas solo por ciberdelitos, ubicándonos en el séptimo lugar de países afectados en la región, según el WEF[30]. La inversión de US$ 22M (veintidós y 00/100 millones de dólares americanos) establecida por el gobierno el año pasado[31] no ha sido suficiente para responder como infraestructura y país ante los ciberataques y sus peligros colaterales. A decir verdad, somos el país con más alto riesgo en América Latina según diversos informes y *journals* especializados[32], centrando nuestra mayor debilidad en el sector público, representado en sus inicios por el ONGEI, y actualmente por el SEGDI. Esto no quiere decir que el sector privado no se encuentre vulnerable ante algún ataque de cualquier tipo, pero el problema radica en que ningún sector en el país está acostumbrado a invertir en seguridad, ni siquiera es una prioridad o básica corporativa, ni maneja un sistema re respaldo con protección adecuada (Zeballos, 2017). No obstante, el mercado de ciberseguridad va creciendo y ronda los US$ 100M (cien y 00/100 millones de dólares americanos), pero solo en el sector privado, una inversión que supera cerca del 500% a la estatal; eso sin contar las áreas de investigación y formación que se vienen propiciando; especialmente, en el sector académico privado, en donde Universidades como la UPC ya genera programas de formación en ciberseguridad, pero que aún no es visto como una carrera profesional, como en países de primer mundo como Japón y EE. UU.

No somos un país avanzado en el sector ciberseguridad. A decir verdad, tenemos un largo trecho sumergidos en la incapacidad para responder ante la realidad global y los peligros que constituye el mal uso de la tecnología. WannaCry (2017), el ransomware que modifico el pensamiento y el accionar de muchos especialistas en seguridad, que marcó un antes y un después en sistema de ataques y recompensas, debió habernos hecho reaccionar como Estado e impulsarnos a la gestación de iniciativas en ciberseguridad. La

[30] Cfr. REDACCIÓN GESTIÓN (2017). **«Perú registrará US$ 4,782 millones en pérdidas por ciberdelitos en 2017»**. Del portal Gestión, sección *Tecnología*. Sitio web: https://gestion.pe/tecnologia/peru-registrara-us-4-782-millones-perdidas-ciberdelitos-2017-141411

[31] **Ibid.**

[32] De acuerdo con el último informe de Rapid7 Labs, **«National Exposure Index»** (2017), el Perú ocupa el puesto 29 a nivel global y segundo en la región, solo superado por El Salvador; sin embargo, nuestra población en Internet es mayor, contando con mayor exposición. La empresa ESET, en su informe **«ESET Security Report Latinoamérica 2017»**, señala que el Perú se encuentra en la lista de los países con más incidentes de phishing en la región, con un 16.6% y solo superado por Ecuador, con un 20.9%. Otro informe importante es el **«Kaspersky Security Network»** (BBC, 2016), ubicándonos en el segundo lugar de países más amenazados por malware, con un 41.9%, solo superados por Brasil, con un 49.9%, siendo más resaltante el que Brasil se encuentre en el TOP 10 de los países mejor preparados contra ciberataques (WEF, 2015).

realidad, es otra. Y con ello en paso, no será extraño afirmar que el Perú no se encuentra preparado para afrontar un mal tan latente y actual como lo es el ciberterrorismo. Estamos lejos de ser un país maduro y consiente en estos temas.

1.1.1.4.1. ¿En qué momento ingresó el crimen a Internet?

No hay una fecha cierta. Tampoco podemos decir que Internet generó el cibercrimen, como se escucha de la labia de algunos juristas que no perciben la realidad del asunto. El cibercrimen nació cuando el hombre comprendió el poder de Internet y las tecnologías. Repito, no hay una fecha concreta, pero sí un conglomerado de fechas conocidas con sus respetivos ciberataques, lo que no nos determina con exactitud cuándo empezó esta historia.

1.1.1.4.2. ¿Qué es un ciberdelito?

He aquí otro punto de discusión, que considero el talón de Aquiles de la ideología peruana frente a la criminalidad cibernética y la preparación jurídico-armamentista a la que nos enfrentamos.

Si preguntamos qué se entiende por ciberdelito, lo más probable es que la respuesta tradicionalista dirá que **«son delitos generados por computadora(s)»**; que, si es interpretado de manera literal, nos llevaría a pensar que nuestras máquinas se levantarán en una revolución, lo cual no ha sucedido hoy en día, pero que de suceder tampoco puede llamársele ciberdelito.

Otra corriente dirá que **«son los delitos que se configuran a través del uso de las máquinas o la tecnología»**, lo cual puede tener cierta lógica, pero se olvida del Internet, que si bien es parte de la tecnología no cuaja en el concepto de los que afirman esta supuesta realidad.

El principal problema es que **«no se entiende lo que es un ciberdelito»**, y es a raíz de esto es que incluso se pretende legislar bajo el tradicionalismo algo que a gritos exclama una actualización jurídica y una preparación en el nuevo campo. Para comprender qué es un ciberdelito, no basta con entender qué es un delito en sí; hay que conocer sobre la tecnología y el mundo para poder llegar a la conclusión y así saber y entender de lo que estamos hablando y de lo que estamos dispuestos a legislar.

1.1.1.4.2.1. *Individualización de los conceptos básicos para comprender la problemática en el mundo actual y el desarrollo de su legislación*

Como ya se señaló, la mayor dificultad con la que cuentan los juristas peruanos —y muchos tradicionalistas de la región— es la imposibilidad de conceptualizar un ciberdelito, mucho más allá de su variedad. Comprender el ciberdelito es ir más allá del concepto de delito, se hace necesario individualizar ciertos conceptos para comprender para comprender el todo de esta vertiente y así suprimir la dificultad latente en nuestra idiosincrasia jurídica, una que tenga como fruto una Ley que abarque la problemática y nos defienda ante los peligros que existen en nuestra generación, diferente con la que convivimos hoy en día.

En primera instancia, no debemos olvidar que el delito es toda conducta **«típica, antijurídica, culpable y punible»** que deriva en una sanción penal. A su vez, esto genera dos tipos de sujetos (activo y pasivo), una acción o acto, y una omisión o conducta.

En segunda instancia, hay que recordar que la ley es la que nos especificará la conducta antijurídica y punible, ya que no podemos sancionar a todos los delitos de la misma manera ni juzgar de la misma manera a sus actores. Por otro lado, recalcar que no necesariamente todo aquello que es considerado delito dentro de nuestro Estado será delito lejos de nuestra territorialidad. He aquí el dilema de Internet, que no tiene territorialidad.

En última instancia, vienen los ciberdelitos, que pueden ser entendidos como la ecuación que tiene el concepto de delito sumado al mundo de Internet y las TIC. Un concepto básico, de fácil entendimiento, pero no del todo cierto, ya que el mundo del ciberdelito se adapta a la concepción social interconectada con la tecnología, lo que nos llevaría a pensar que una norma que fue diseñad por los hombres y para los hombres, finalmente no podrá juzgar a una IA en un futuro no muy lejano.

Pero los ciberdelitos no son más que la evolución del delito mismo en el campo social moderno. Su amenaza es mayor, no cabe duda, por lo que no podemos verlos como delitos comunes.

Son muchos los que han dado su concepto de ciberdelito. Los sectores públicos, privados, académicos y sociedad civil se han pronunciado en distintos momentos, dejando en claro que el concepto de ciberdelito varía con el paso del tiempo.

De ese modo, tenemos el término presentado por un grupo de expertos invitados por la OCDE (Francia, 1983) en donde se relacionó la definición de delito con los computadores, para dar paso a un concepto que se concreta como **«cualquier comportamiento antijurídico, no ético o no autorizado, relacionado con el procesado automático de datos y/o transmisiones de datos»**, dando paso a un concepto que permite la facilidad de trabajo con los estudios penales, legales, criminológicos y otras variantes.

El reconocido jurista alemán Klaus Tiedemann, hablaría también de los ciberdelitos en 1985. Para él, **«aquél (delito) en el que para su comisión se emplea un sistema automático de procesamiento de datos o de transmisión de datos»**[33], estableciendo la necesidad de estos instrumentos para considerarlo como actos antijurídicos según la ley penal.

En 1997, a razón de los primeros debates sobre la primera Ley de ciberdelitos en el Perú, el jurista Luis Bramont–Arias afirmaría que **«no existe un concepto de delito informático**[34] **—computer crime o *computerkriminalität*— que sea aceptado por el derecho penal de manera unánime debido a que la delincuencia informática comprende una serie de comportamientos que es difícil reducir o agrupar en una sola definición»**[35]. A pesar de lo expuesto, esto no sería tomado en cuenta durante el desarrollo de la primera norma, la cual solo consideró a los ciberdelitos como acciones que perjudican a los usuarios de la banca, desprotegiendo a otras personas que sería víctimas de delitos que no se configuraban en esa Ley; como, por ejemplo, la suplantación de identidad.

[33] TIEDEMANN, Klaus (1985). **«Poder económico y delito: introducción al derecho penal económico y de la empresa»**. Pp.121-122. Barcelona, España. Editorial Ariel.

[34] Denominación con la que muchos discrepamos hasta hoy en día, toda vez que da una connotación diferente a la problemática que tratamos y parece solo referirse a la información y no al globo de Internet, TIC y sus variables.

[35] BRAMONT–ARIAS TORRES, Luis (1997). **«El Delito Informático en el Código Penal Peruano»**. Pp.27. Fondo Editorial de la Pontificia Universidad Católica del Perú. Lima, Perú.

Para 1999, el estudioso español Carlo Sarzana se pronuncia alegando que **«cualquier comportamiento criminógeno en el cual la computadora ha estado involucrada como material o como objeto de la acción criminógena, o como mero símbolo»**[36] llega a ser considerado un ciberdelito. Hasta este momento, y casi al cierre del milenio, la presencia de las computadoras sigue siendo considerado como factor único al hablar de este tipo de crímenes.

El nuevo milenio trajo consigo una rápida evolución de las tecnologías. Superado el rumor del reseteo del año 2000, en donde se rumoraba sobre el descontrol de la máquina y la perdida de la información, se dio paso a nuevas visiones y creaciones; y dentro de esta amalgama de conocimiento, el Derecho dio paso a conceptualizaciones más modernas del ciberdelito.

Es así como en el 2008 Miguel Ángel Davara Rodríguez, jurista español, define a los ciberdelitos como **«la realización de una acción que, reuniendo las características que delimitan el concepto de delito, sea llevada a cabo utilizando un elemento informático y/o telemático, o vulnerando los derechos del titular de un elemento informático, ya sea hardware o software»**[37], lo que dio paso a la comprensión el software como parte de un todo, susceptible de manipulación o como herramienta para la criminalidad.

Julio Téllez, jurista mexicano, relanzó un nuevo concepto para el 2009. El investigador definió a los ciberdelitos como **«son actitudes ilícitas que tienen a las computadoras como instrumento o fin (concepto atípico)" o las "conductas típicas, antijurídicas y culpables que tienen a las computadoras como instrumento o fin (concepto típico)»**[38],

Las empresas de seguridad también han participado con la conceptualización de los ciberdelitos. Una es la empresa de seguridad AVAST®, afirmando que

[36] SARZANA, Carlo (1999). **«Criminalità e tecnología: Computer crime»**. Pp.53. Roma, Italia. Rassagna Penitenziaria e Criminología.

[37] DAVARA RODRÍGUEZ, Miguel Ángel (2008). **«Manual de Derecho Informático»**. Pp. 358-359. Pamplina, España. Editorial Thomson–Aranzadi.

[38] TÉLLEZ VALDÉZ, Julio (2009). **«Derecho Informático»**. Pp. 188. México DF, México. McGRAW-HILL/INTERAMERICANA EDITORES S.A.

«el ciberdelito constituye ahora una amenaza mayor que nunca, ya que cada vez más usuarios están conectados a Internet a través de equipos portátiles, smartphones y tablets. Por ello, es una de las actividades ilegales más rentables. El ciberdelito se puede presentar de multitud de formas, que a grandes rasgos se pueden dividir en dos categorías: "delitos puntuales", como instalar un virus que robe su información personal; o "delitos recurrentes»", como el ciberacoso, la extorsión, la distribución de pornografía infantil o la organización de ataques terroristas». Este es un concepto más avanzado que incluye mayores conductas que guardan relación con la realidad, así como elementos a través de los cuales se ejecutan los ataques o se llegan a las víctimas. Un concepto más completo, pero no el único-

El Departamento de Justicia de EE. UU. mantiene su propia definición de ciberdelito, señalando que es **«cualquier acto ilegal en relación con el cual el conocimiento de la tecnología informática es esencial para su comisión, investigación y persecución»**. Este concepto no habla de hardware o software, y ha llegado a ser el más aceptado por especialistas de todo el mundo, ya que comprende que la tecnología es innovación, y como tal, no puede mantenerse estática a un solo componente, lo que podría dar paso —en un futuro cercano— a la penalización de conductas realizadas por IA.

La actual Ley de ciberdelitos de Perú (Ley N°30096) también ha brindado su concepto de ciberdelito, considerándolo como **«conductas ilícitas que afectan los sistemas y datos informáticos y otros bienes jurídicos de relevancia penal, cometidas mediante la utilización de tecnologías de la información o de la comunicación»**, que para muchos ha resultado ser un concepto limitante, y comprobaremos el por qué más adelante.

Si bien es cierto que existe una infinidad de conceptos —y muchos de ellos no pueden soltar al hardware y software de su apreciación—, es muy probable que hoy en día siga sin una figura verás que precise lo que es un ciberdelito. Es la evolución del delito mismo —como ya se explicó—, una figura adaptable al denominador social actual, la sociedad y la generación interconectada y *tecnodependiente*.

La dificultad mayor para un concepto estático radica en el avance del mundo, las TIC e Internet, tres elementos fundamentales que, asociados al actuar del hombre —componente indispensable en toda figura delictiva— conlleva a innovación o destrucción, de acuerdo con el uso de las habilidades.

Podemos discutir sobre como cada legislación comprende el problema del ciberdelito; aun así, existiría un debate pues consideraríamos que la realidad normativa no es coherente a la realidad misma. Esto, muchas veces —y uno de los casos es nuestro—, se debe a que se deja en manos de desconocedores en la materia un trabajo tan delicado. Incluso en nuestro país, a pesar de los informes, noticias y foros de trabajo, no se ha llegado a aceptar a los ciberdelitos y la ciberdelincuencia como la amenaza más grave actualmente conocida. Poco o nada podemos decir del ciberterrorismo, el cual aún rechazan su existencia.

1.1.1.4.2.2. *Figuras ciberdelictivas*

Este es otro de los problemas base que existe al momento de hablar de ciberdelitos y su lucha legal. Cierto sector del periodismo —en base a desconocimientos y poca investigación— ha llegado a fusionar conceptos que nos pasan factura en la actualidad, cuando más trabajo tenemos en frente. Muchos errores para identificar personajes y responsables, así como sus actividades, cala también en el sector jurídico. Es por ello por lo que en estos últimos años se ha visto en la necesidad de aclarar estas terminologías, con el fin de acabar con los mitos que —erradamente y a propósito— se han propagado en la sociedad y dificultan el trabajo legislativo.

1.1.1.4.2.2.1. **Crackers**

Un *cracker* es un entusiasta de la tecnología, una persona que utiliza habilidades de *hacker* para fines ilícitos —en su mayoría destructivos—, sea obteniendo acceso no autorizado a un sistema o red, destruirlo y/o robar/suprimir información personal o crediticia —previa vulneración de seguridad—.

entre otras acciones. Este término proviene del inglés *crack* que significa romper o quebrar.
También se considera *cracker* a la persona que modifica un software para utilizarlo sin las limitantes de licencia, populares en el mundo de los videojuegos del mercado negro; pero este no es el término necesitado para la investigación, y muchas veces, ni siquiera es tomado en cuenta para acciones publicitarias.

Lo que debe queda en claro es que el *cracker* es el verdadero ciberdelincuente y amenaza dentro de la red; y no el *hacker*, como muchas veces se ha expresado y ha querido demostrarse de manera errada.

1.1.1.4.2.2.2. Cybercrooks

El término *cybercrook* no es muy conocido por la comunidad jurídica, por lo que su uso es extremadamente limitado; sin embargo, es parte de la figura ciberdelictiva existente en la actualidad.

Para algunos, hablar de *cybercrook* es hacer referencia a un sinónimo para ciberdelincuentes. Por otro lado, el diccionario Oxford se refiere a este como cibercriminal, una persona que realiza actividades con fines ilícitos empleando Internet y las computadoras para ingresar ilegalmente a los sistemas. Y si bien se mantiene este concepto, su figura puede ser confundida con un *cracker*, pero se le relaciona más con un intruso de sistemas que con un rompedor de firewalls.

1.1.1.4.2.3. *Figuras de ciberseguridad*

Dos términos son los que se emplean más en la actualidad. Uno, en una dirección errada, y el otro, en una dirección proyectada al orden público. No obstante, ambas son figuras del orden que se manejan en dos dimensiones diferente —una tradicional y la otra moderna— con similares objetivos.

1.1.1.4.2.3.1. Hackers

Es necesario decir que durante años —incluso, hasta hoy— el término *hacker* ha sido mal utilizado por los medios de comunicación y personas

desconocedoras en el tema —entre ellos, gran parte del sector jurídico nacional—. Se ha enclaustrado su personalidad en la de un delincuente, una persona que utiliza sus habilidades para fines ilícitos, pero todo está más alejado de la realidad que de costumbre.

Un *hacker* es una persona con amplio conocimiento de las TIC e Internet, y que utiliza sus habilidades para potenciar la seguridad de las empresas, estado y todo aquel que necesite de su ayuda. Su actividad es conocida como *ethical hacking* —también conocido como *penetration testing*—, tiene como objetivo explotar las vulnerabilidades existentes en el sistema de interés valiéndose de test de intrusión, que verifican y evalúan la seguridad física y lógica de los sistemas de información, redes de computadoras, aplicaciones web, bases de datos, servidores, etc., con la intención de ganar acceso y demostrar que un sistema es vulnerable, obteniendo información de gran ayuda para las organizaciones al momento de tomar las medidas preventivas en contra de posibles ataques malintencionados (UNAM-CERT, 2011).

Las pruebas de penetración se enfocan principalmente en las siguientes perspectivas[39]:

- **Pruebas de penetración con objetivo:** se buscan las vulnerabilidades en partes específicas de los sistemas informáticos críticos de la organización.
- **Pruebas de penetración sin objetivo:** consisten en examinar la totalidad de los componentes de los sistemas informáticos pertenecientes a la organización. Este tipo de pruebas suelen ser las más laboriosas.
- **Pruebas de penetración a ciegas:** en estas pruebas sólo se emplea la información pública disponible sobre la organización.
- **Pruebas de penetración informadas:** aquí se utiliza la información privada, otorgada por la organización acerca de sus sistemas informáticos. En este tipo de pruebas se trata de simular ataques realizados por individuos internos de la organización que tienen determinado acceso a información privilegiada.

[39] REYES PLATA, Alejandro (2011). **«Ethical Hacking»**. 2017, de UNAM-CERT. Sitio web: https://www.cert.org.mx/historico/documento/index.html-id=7#Types

- **Pruebas de penetración externas:** son realizas desde lugares externos a las instalaciones de la organización. Su objetivo es evaluar los mecanismos perimetrales de seguridad informática de la organización.
- **Pruebas de penetración internas:** son realizadas dentro de las instalaciones de la organización con el objetivo de evaluar las políticas y mecanismos internos de seguridad de la organización.

A su vez, cada tipo de pruebas descrito anteriormente se puede ubicar en dos modalidades dependiendo si el desarrollo de las pruebas es de conocimiento del personal informático o no.

- **Red Teaming:** Es una prueba encubierta, es decir que sólo un grupo selecto de ejecutivos sabe de ella. En esta modalidad son válidas las técnicas de ingeniería social para obtener información que permita realizar ataque. Ésta obviamente es más real y evita se realicen cambios de última hora que hagan pensar que hay un mayor nivel de seguridad en la organización.

- **Blue Teaming:** El personal de informática conoce sobre las pruebas. Esta modalidad se aplica cuando las medidas tomadas por el personal de seguridad de las organizaciones ante un evento considerado como incidente, repercuten en la continuidad de las operaciones críticas de la organización, por ello es conveniente alertar al personal para evitar situaciones de pánico y fallas en la continuidad del negocio.

1.1.1.4.2.3.2. Ciberpolicía

También llamada policía cibernética, en una institución creada para realizar patrullaje en Internet y así detectar sitios maliciosos, procesos y/o responsables de conductas delictivas, entre otras actividades maliciosas que puedan generarse en la red, todas ellas generadas a través del apoyo de las TIC. Adicional a ello, brinda información a la ciudadanía sobre los peligros que pueden darse con Internet y el uso de las tecnologías, y como actuar si se ha sido víctima de un hecho delictivo, como el proceso de presentación de denuncia. Asimismo, la

policía cibernética colabora con el Ministerio Público, de así ser requerido para investigaciones.

Al igual que en el mundo físico, esta nueva modalidad de patrullaje busca prevenir múltiples delitos que se vienen produciendo en Internet, no limitando su actividad a hechos ya producidos, todo bajo el anonimato.

En el Perú, la DIVINDAT cumple la labor de una ciberpolicía.

1.1.2. *Sobre las normas materia de ciberdelitos que rigieron y rigen en el Perú: Historia de una problemática legislativa*

La realidad peruana a razón de los llamados ciberdelitos siempre se ha mantenido ajena no solo a la realidad social nacional, sino también internacional. De ahí que los principales reportes emitidos por organizaciones tales como la OEA[40] no nos califican como referentes; muchos menos en las reuniones de los capítulos de IGF locales[41] o ISOC PERÚ[42], en donde esta materia no se trata en los diálogos. Y si de estrategias de ciberseguridad se trata, lo más cercanos que llevamos en los últimos años son las discusiones para determinar si la DINI debe velar por la ciberseguridad del país o dar a creación una nueva institución, sin medir en cuenta que hay otros factores de igual importancia —y complementarios— a tratarse, tales como la modificación legislativa, el apoyo en la academia, entre otros[43]. Puedo dar fe que, con cerca de 10 años

[40] Cfr. BANCO INTERAMERICANO DE DESARROLLO Y LA ORGANIZACIÓN DE ESTADOS AMERICANOS (2016). Documento **«Ciberseguridad: ¿Estamos preparados en América Latina y el Caribe?»**. Obra sujeta a licencia CreativeCommons IGO 3.0 Reconocimiento-NoComercial-SinObrasDerivadas (CC-IGO 3.0 BY-NC-ND) (http://creativecommons.org/licenses/by-ncnd/3.0/igo/legalcode)

[41] De acuerdo con su portal web, http://gobernanzadeinternet.pe/, El Foro de Gobernanza de Internet Perú tiene como objetivo establecer un espacio de diálogo sobre Gobernanza de Internet en el cual los distintos representantes del gobierno, la sociedad civil, la academia, la comunidad técnica y el sector privado dialoguen sobre el uso y desarrollo de Internet en el Perú. Este espacio busca favorecer la participación informada de los actores del país en foros regionales e internacionales sobre el mismo tema como el Foro de Gobernanza de Internet (IGF) y el Foro Latinoamericano de Gobernanza de Internet (LACIGF). A la fecha, no se ha mantenido registro de foros que hayan permitido el dialogo de materias tales como ciberseguridad y ciberdelitos, como sí están presenten en los IGF locales de otros países de la región.

[42] ISOC Perú es uno de los capítulos de la región pertenecientes a la organización internacional sin fines de lucro Internet Society (ISOC), y si bien, no es función de ISOC centrarse en aspectos tan resaltantes como la ciberseguridad, si propicia —y participa en— las reuniones donde se dialoga sobre esta materia, comprendiendo también que tenerla en el mapa de desarrollo de Internet es fundamental. Es importante resaltar que luego de muchos años ISOC Perú vuelve a participar en las principales reuniones en materia de Gobernanza de Internet, llegando con expectativas que la comunidad digital peruana espera que cumplan.

[43] El 14 de diciembre de 2016, se presentó el Proyecto de Ley N°722/2016-CR, que modifica los artículos 2°, 10°, 17°, 38° y la incorporación de la Octava Disposición Complementaria Final del Decreto Legislativo N°1141, Decreto Legislativo de fortalecimiento y modernización del Sistema de Inteligencia Nacional-SINA y de la Dirección Nacional de Inteligencia-DINI, presentada por la bancada del partido Fuerza Popular e

de investigación en la materia, el gran avance hasta el momento es la Ley N°30096 – Ley de delitos informáticos en el Perú, y su modificatoria, Ley N°30171, ambas calificadas como poco realistas y con tantos vacíos legales que complica la labor tanto de abogados como de fuerzas policiales para ir tras los delincuentes.

No somos México, país que viene debatiendo una Estrategia Nacional de Ciberseguridad (ENC), la cual mantuvo una constante consulta a su población y en donde expertos nacionales e internacionales, así como representantes del sector privado, de la industria, sociedad civil, gobierno, órganos autónomos constitucionales, comunidad técnica y academia.[44], No somos Estonia, Israel, República de Corea o Estados Unidos, ejemplos claros de políticas y prácticas de ciberseguridad, quienes tienen claro la importancia de la educación y la cultura, así como las adaptaciones legales al nuevo tiempo[45]. No somos España, quienes no solo cuentan con una ENC desde el 2013[46]; sino que, además, avanzan cada día más en el trabajo colaborativo, y en el que su Ministerio de Asuntos Exteriores y de Cooperación trabaja en distintos ámbitos internacionales en la Ciberseguridad[47]. **«No somos como muchos países y estamos lejos de tomarlos siquiera como ejemplo»**. Para ser realistas, el Perú, en material legal de ciberdelitos —que guarda plena relación con la dinámica de la ciberseguridad— hace un enfoque burdo y hasta incluso permisivo con el ciberdelincuente, sin dejar en claro siquiera qué pensaban los que estuvieron detrás de la producción de nuestras actuales leyes, ni mucho menos que querían lograr con estas. Podría interpretarse, incluso, que el enfoque digital/cibernético en materia del Derecho es un enfoque que no debe de dársele «la menor importancia». De no ser así, no creo que hubiéramos vivido por diecisiete años con una legislación que no solo era permisiva, sino que solo permitía la penalidad de un único ciberdelito y dejaba de lado los restantes, los que se centraban en la banca.

---

iniciativa del congresista **MARCO ENRIQUE MIYASHIRO ARASHIRO**. El 27 de julio de 2017, y luego de múltiples mesas de trabajo, se publica de manera oficial la Ley N°30618, Ley que modifica el Decreto Legislativo 1141, decreto legislativo de fortalecimiento y modernización del Sistema de Inteligencia Nacional - SINA y de la Dirección Nacional de Inteligencia - DINI, a fin de regular la seguridad digital, donde se establecen las funciones principales del SINA y la DINI, conceptos como seguridad digital, entre otros. No obstante, no hay una discusión relacionada a la ley de ciberdelitos vigentes ni mucho menos discusiones más resaltantes en materia de ciberseguridad.

[44] Cfr. ORGANIZACIÓN DE ESTADOS AMERICANOS Y LA PRESIDENCIA DE LA REPÚBLICA DE MÉXICO (2017). Documento **«Hacia una estrategia nacional de ciberseguridad: Consolidación de las consultas a actores nacionales»**.

[45] Cfr. BANCO INTERAMERICANO DE DESARROLLO (2016). Documento para discusión N°IDB-DP-457 **«Experiencias avanzadas en políticas y prácticas de ciberseguridad: Panorama general de Estonia, Israel, República de Corea y Estados Unidos»**. Obra sujeta a licencia CreativeCommons IGO 3.0 Reconocimiento-NoComercial-SinObrasDerivadas (CC-IGO 3.0 BY-NC-ND) (http://creativecommons.org/licenses/by-nc-nd/3.0/igo/legalcode)

[46] Cfr. PRESIDENCIA DEL GOBIERNO DE ESPAÑA (2013). **«Estrategia de ciberseguridad nacional»**.

[47] GOBIERNO DE ESPAÑA - Ministerio de Asuntos Exteriores y de Cooperación. **«Ciberseguridad y cooperación Internacional»**. Información detallada en el documento recuperado: http://www.exteriores.gob.es/Portal/es/PoliticaExteriorCooperacion/Ciberseguridad/Paginas/Ciberseguridad-y-Cooperaci%C3%B3n-Internacional.aspx

Para entender —o buscar entender— el enfoque del legislador peruano es necesario hacer un análisis sobre la primera norma por la cual nos regimos, los proyectos de Ley, la Resolución Directoral que crea a la DIVINDAT; así como la controversial actual ley de ciberdelitos —mal llamados, delitos informáticos— de nuestro país.

1.1.2.1. ***Sobre la Ley N°27309 – Ley que incorpora los delitos informáticos al código penal***

La **LEY N°27309**[48], publicada el 17 de julio de 2000, fue la primera Ley vigente en el Perú que hacía referencia a los mal llamados delitos informáticos. Los artículos que la componían se encontraban en el Código Penal, en las numeraciones 207°-A[49], 207°-B[50], 207°-C[51] y 208°[52], y aunque las dos primeras incluyeran los tipos de delitos y los dos restantes se mantuvieran en el margen de agravantes, la mencionada Ley enclaustraba a los ciberdelitos solo en el **AMBITO DE HURTO AGRAVADO**.

Durante aproximadamente diecisiete (17) años, el Perú vivió el régimen de una Ley de ciberdelitos que no cubría ni el diez por ciento (10%) de los delitos existentes hasta ese entonces, como la pornografía infantil en el ámbito de Internet, tráfico de datos, entre otros.

---

[48] Esta Ley modificó el Título V (Delitos Contra el Patrimonio) del Libro Segundo (Parte Especial - Delitos) del Código Penal peruano de aquel entonces, y ubicó los mencionados artículos en **CAPÍTULO X - DELITOS INFORMÁTICOS** y el **CAPÍTULO XI - DISPOSICIÓN COMÚN**.

[49] **Artículo 207-A.- Delito Informático**
El que utiliza o ingresa indebidamente a una base de datos, sistema o red de computadoras o cualquier parte de la misma, para diseñar, ejecutar o alterar un esquema u otro similar, o para interferir, interceptar, acceder o copiar información en tránsito o contenida en una base de datos, será reprimido con pena privativa de libertad no mayor de dos años o con prestación de servicios comunitarios de cincuentidós a ciento cuatro jornadas.
Si el agente actuó con el fin de obtener un beneficio económico, será reprimido con pena privativa de libertad no mayor de tres años o con prestación de servicios comunitarios no menor de ciento cuatro jornadas.

[50] **Artículo 207-B.- Alteración, daño y destrucción de base de datos, sistema, red o programa de computadoras**
El que utiliza, ingresa o interfiere indebidamente una base de datos, sistema, red o programa de computadoras o cualquier parte de la misma con el fin de alterarlos, dañarlos o destruirlos, será reprimido con pena privativa de libertad no menor de tres ni mayor de cinco años y con setenta a noventa días multa.

[51] **Artículo 207-C.- Delito informático agravado**
En los casos de los Artículos 207-A y 207-B, la pena será privativa de libertad no menor de cinco ni mayor de siete años, cuando: 1. El agente accede a una base de datos, sistema o red de computadora, haciendo uso de información privilegiada, obtenida en función a su cargo. 2. El agente pone en peligro la seguridad nacional.

[52] **Artículo 208.- Excusa absolutoria. Exención de Pena**
No son reprimibles, sin perjuicio de la reparación civil, los hurtos, apropiaciones, defraudaciones o daños que se causen: 1. Los cónyuges, concubinos, ascendientes, descendientes y afines en línea recta. 2. El consorte viudo, respecto de los bienes de su difunto cónyuge, mientras no hayan pasado a poder de tercero. 3. Los hermanos y cuñados, si viviesen juntos.

A ello mismo, el jurista peruano Luis Alberto Bramont–Arias Torres, en un artículo escrito para la **«Revista Peruana de Derecho de la Empresa»**, en el año 2000, nos comenta que existe una problemática con este fenómeno del uso de las computadoras de manera abusiva y que lleva a la necesidad de recurrir al Derecho Penal a fin de disuadir ese uso abusivo, el mismo que ya se ha plasmado en varias legislaciones extranjeras. (El subrayado es mío).

Por otro lado, y siguiendo dentro de este análisis, luego de explicar detalladamente cada punto, fuerza y debilidad del artículo y sus incisos en mención, Bramont–Arias concluye con lo siguiente:

> «*El delito informático en el Código Penal Peruano ha sido previsto como una modalidad de hurto agravado, lo cual trae inconvenientes, teniendo en cuenta la forma tradicional de comprender los elementos del delito de hurto. Asimismo, existen conductas vinculadas a los delitos informáticos que, en algunos casos, pueden configurar otro tipo de delitos, como, por ejemplo, el delito de daños. A manera de recomendación, sería conveniente la creación de un tipo autónomo que sancione las conductas vinculadas al delito informático*».

Muchos delitos quedaron excluidos de la ya extinta Ley N°27309. De entre la amplia lista de delitos no incluidos en aquel entonces están los mencionados robos de identidad, espionaje, pornografía infantil y, por supuesto, el delito de ciberterrorismo.

Desde este momento de la historia y en adelante, nuestro país, en comparación de otros países de la región como Chile[53], Venezuela[54] o Colombia[55], llevaría un gran atraso con relación a la materia jurídica y a la luca contra los ciberdelitos.

1.1.2.2. ***Sobre la Resolución Directoral N°1695-2005-DIRGEN/EMG-08AGO2005 de la Policía Nacional del Perú (PNP) que crea la División de Investigación de Delitos de Alta Tecnología (DIVINDAT) de la Dirección de Investigación Criminal (DIRINCRI)***

Como era de esperarse, cinco (5) años después de promulgada la primera Ley sobre ciberdelitos nacional, mediante Resolución Directoral **N°1695-2005-DIRGEN/EMG-08AGO2005** se crea la **DIVISIÓN DE DELITOS DE ALTA TECNOLOGÍA (DIVINDAT) de la DIRINCRI**. Esta división de la policía

[53] Véase CHILE: **«Ley N°19223 de 07 de junio de 1993 – Ley que Tipifica Figuras Penales relativas a la Informática»**.

[54] Véase VENEZUELA: **«Ley Especial contra los Delitos Informáticos de Venezuela»**.

[55] Véase COLOMBIA: **«Ley N°1273 de 05 de enero del 2009 – Ley que modifica el Código Penal, creando un nuevo bien jurídico tutelado denominado "de la protección de la información y de los datos»**.

significaría un gran avance en la lucha contra la ciberdelincuencia y el ciberdelito. No obstante, de acuerdo con el análisis jurídico y la realidad de la mencionada Ley, el destino es diferente.
A través del mencionado documento, la DIVINDAT tiene la misión de: Investigar, denunciar y combatir el crimen organizado y otros hechos trascendentes a nivel nacional en el campo de[56]:

- *Delito contra el patrimonio* (Hurto agravado de fondos mediante sistemas de transferencias electrónicas de la telemática en general).
- *Delito contra la libertad - Ofensas al pudor público (pornografía infantil)*, en sus diversas modalidades.

Es lamentable percatarse que, existiendo una división de la DIRINCRI encargada de luchar contra el cibercrimen y la ciberdelincuencia desde el año 2005, ésta haya tenido que trabajar durante ocho (8) años luchando contra delitos que ni el mismo legislador consideraba como tales en las normas señaladas en aquella época —en referencia a la Ley N°27309 y los artículos 207°, incisos del A–C, y el artículo 208° del Código Penal peruano—; delitos como las amenazas por e-mail; pornografía infantil en internet; chantaje sexual y económico; intrusiones a sistemas; entre otros, que han gozado del triste privilegio de no ser considerados **«conductas sancionables en nuestro país»**.

La Ley de aquel entonces le jugaba una mala pasa a la DIVINDAT, puesto que, al no sancionar y no señalar como conductas punibles aquellos delitos contra los que luchaba la mencionada división de la DIRINCRI, generó consigo un gran vacío legal aprovechado por los criminales, pues debemos recordar que **NADIE ESTÁ OBLIGADO A HACER LO QUE LA LEY NO MANDA NI DEJAR DE HACER LO QUE LA LEY NO PROHÍBE**. Con ello, se generó la primera ventaja para el hampa en referencia a esta modalidad delictiva en nuestro país.

1.1.2.3. ***Sobre los Proyectos de Ley 034/2011-CR; 307/2011-CR y 1136/2011-CR y su propuesta dentro del ámbito de los ciberdelitos***

El 26 de junio de 2012 el Poder Legislativo acordó por mayoría la aprobación de un texto sustitutorio proveniente de los **PROYECTOS DE LEY 034/2011-CR**, **307/2011-CR** y **1136/2011-CR**, lo mismos que proponían la modificación de los artículos del Código Penal de aquel entonces (Art.207°-A, 207°-B, 207°-C y 208°), derivados de la Ley N°27309, adaptando de esta manera las sanciones y los delitos a los nuevos avances de la

[56] **Historia de la División de Delitos de Alta Tecnología de la DIRINCRI (DIVINDAT)**. A través de la página en mención se hace un informe de las labores que realiza dicha unidad. En: https://www.pnp.gob.pe/direcciones/dirincri/divisiones/historiaDivindat.html

sociedad y en donde se dejaba en claro cuáles eran y deberían ser los ciberdelitos sancionables en nuestro país.

La lista de aquel entonces proponía delitos como el sabotaje informático, pornografía infantil, intrusismo informático, delito informático contra la intimidad y el secreto de las comunicaciones, hurto, obtención indebida de bienes o servicios, falsificación de documentos, entre otros.

El texto presentado constituye un compendio de diferentes libros y diferentes autores, pero su estructura, más que brindar una propuesta acorde a la realidad global, terminó siendo un ***copy-paste mal elaborado*** de diversos trabajos realizados por catedráticos y especialistas internacionales. Este proceso forjó una visión un tanto trágica y deplorable, un trabajo que obligaba una reformulación por el bien de la sociedad y los usuarios de la red de redes. Además, por si el plagio no fuera suficiente, los proyectos de Ley presentados guardan artículos que tienen a malas interpretaciones y que han generado vacíos que podrían ser ventajosos para el crimen. Realidad que sí se produjo una vez se presentara la Ley oficial.

1.1.2.4. ***Sobre la Ley N°30096 – Ley de delitos informáticos en el Perú***

Fruto de los cuestionados Proyectos de Ley, el 12 de septiembre de 2013 se aprueba la promulgación de esta nueva norma. No obstante, no es hasta el 23 de octubre del mismo año que esta nueva Ley entra en vigor, derogando la Ley N°27309 y los artículos que de ella se componen.

La **LEY N°30096–LEY DE DELITOS INFORMÁTICOS** llevó al Perú a la tan ansiada evolución y actualización del delito, dándonos un nuevo enfoque y un nuevo panorama dentro del ambiente de los mal llamados delitos informáticos; sin embargo, aunque el enfoque de señalar a los ciberdelitos como hurto agravado ya se ha superado, el nuevo problema radica en las penas impuestas a aquellos que cometen delitos en el campo digital y mediante el uso de las TIC, siendo lo suficientemente dóciles; y en algunos casos, brindando vacíos que pueden ser aprovechados por los ciberdelincuentes. Por brindar un ejemplo de lo señalado en el presente texto, **«quienes contacten con menores de hasta 14 años con fines sexuales serían sancionados con una pena de prisión de cuatro a ocho años»**[57], una sanción que no justifica la pena ante tan abominable paso que conlleva a la pornografía infantil e incluso peor, a la trata de personas, **«negocio»** que ha tenido un mayor

[57] *Palabras del Presidente de la Comisión de Justicia, Juan Carlos Eguren, explicando la propuesta legislativa y sus diferentes sanciones a los diversos delitos informáticos*. DIARIO EL COMERCIO. Sección Política. **«Los delitos informáticos serán castigados con pena de cárcel»**. Artículo publicado el 13 de septiembre de 2013. Lima – Perú.

alcance con el apoyo de la DEEP WEB, DARK WEB y el *e-commerce* con bitcoins, tramos que la actual ley no discute.

Siguiendo con la dinámica de nuestra legislación vigente, de los delitos que se conocen, el presidente de la Comisión de Justicia del Perú, Juan Carlos Eguren, siguió su pronunciamiento señalando que[58]:

- Si una persona sin autorización afecta datos informáticos o de usuario, el funcionamiento de un sistema o una red informática o de telecomunicaciones, recibirá una pena privativa de la libertad no menor de tres ni mayor de seis años.
- Quienes cometan delito contra la intimidad y el secreto de las comunicaciones en el ámbito informático recibirá no menos de dos ni más de cinco años de prisión. Si esta figura es agravada, la pena oscilará entre cinco y diez años de cárcel.
- Para aquellos que incurran en la interceptación de información clasificada como secreta, confidencial y que comprometa la seguridad nacional, se establecen penas privativas de la libertad de ocho a diez años de prisión.
- Aquellas personas que desarrollen y distribuyan programas que faciliten el acceso ilícito a datos informáticos recibirán una pena que va entre uno a cuatro años de prisión.

Lo cierto es que esta Ley ha causado muchos problemas para el Derecho y la sociedad desde su promulgación, en especial al llevarnos a suponer si la conducta es dolosa o culposa, o que no tengamos la manera de cómo identificar al responsable del delito. A pie cito uno dos artículos de la Ley N°30096 que, a mi parecer, son las dos más llamativas de esta nueva norma.

> ***Artículo 3° – Atentado contra la integridad de datos informáticos***
> *El que, a través de tecnologías de la información o de la comunicación, introduce, borra, deteriora, altera, suprime o hace inaccesibles datos informáticos, será reprimido con pena privativa de libertad no menor de tres ni mayor de seis años y con ochenta a ciento veinte días multa.*

Durante una cátedra ofrecida por mi persona en el año 2013 para dos reconocidas universidades del país, ambas impartidas para el curso de Derecho Informático, se dialogó mucho sobre este artículo, las incongruencias y el peligro que significaría para con la ciudadanía en general, pero especialmente, con el futuro del Estado.

En ningún momento el artículo especifica si el daño se puede producir por **DOLO** o por **CULPA**, y como debería de ser tratado

[58] **Ibid.**

en ambos casos, quedando en manos de quien la interpreta una de las múltiples respuestas. Por otro lado, se genera el gran vacío: **«¿Qué pasaría si introduzco, borro, deterioro, altero, suprimo o hago inaccesibles datos informáticos, pero siendo yo el dueño de aquella información?»**, **«¿Se me puede llevar a la cárcel?»** La persona que realiza estas acciones, en una especie de acto *altruista*, **«¿puede denunciarse a sí misma?»** Si de manera equivocada descargo un mail del trabajo y este contenía un malware que daña la información o genera espionaje, **«¿es enteramente mi culpa?»**, **«¿la culpa es de quién diseño el malware?»**, **«¿la empresa en la que trabajo tendrá alguna responsabilidad?»**, **«¿esto me obligará a tener equipos de respuestas?»**

Estas son algunas de las muchas preguntas saldrían a la luz, pero este no es parte del tema de la Tesis. Sin embargo, sirve para explicar cómo es el que el legislador ha generado un vacío por diversos motivos que incluso nosotros, ciudadanos peruanos, desconocemos hasta la fecha.

Por otro lado, el siguiente artículo es uno de los que, a mi percepción, puede considerarse peligroso en potencia.

> ***Artículo 9° – Suplantación de Identidad***
> *El que mediante las tecnologías de la información o de la comunicación suplanta la identidad de una persona natural o jurídica, siempre que de dicha conducta resulte algún perjuicio, material o moral, será reprimido con una pena privativa de la libertad no menor de tres ni mayor de cinco años.*

Este quizás sea, junto a la figura del ciberterrorismo, uno de los mayores males de la estructura de Internet y cuyos efectos se perciben tanto en el ciberespacio como en el mundo real. Uno de los casos más emblemáticos en *suplantación de identidad* es el de Ruth Jeffrey, una estudiante universitaria de Reino Unido que, si bien su calvario inició con un acoso cibernético —su caso fue noticia en Inglaterra en 2011—, la derivación de este primero delito —que además no está penalizado en nuestro país—, llevó al acosador a la **SUPLANTACIÓN DE IDENTIDAD**, afirmando ser ella en las redes sociales, y colocando/compartiendo fotografías de ella desnuda, destruyendo su imagen de alumna modelo y ejemplar, así como su autoestima e integridad como ser humano.

Durante tres años y medio Ruth Jeffrey fue sometida a abuso emocional y mental a manos de un acosador desconocido, traumas que empeoraron y que estuvieron a punto de llevar al suicidio cuando se postearon imágenes de ella en sitios web para adultos y se distribuyeron entre sus familiares y amigos.

El caso de Ruth Jeffrey es uno de tantos que demuestra, de forma clara y real, que la visión del legislador peruano, al momento de formular el controversial Artículo N°9 no pensó en un punto tan clave como las intenciones del robo de identidad. **NADIE ROBA O SUPLANTA LA IDENTIDAD DE UNA PERSONA SIN UNA INTENCIÓN MALICIOSA. EL ROBO Y LA SUPLANTACIÓN DE IDENTIDAD, SEA CUÁL SEA SU MOTIVACIÓN, SIEMPRE ES UN DELITO QUE PERJUDICA TANTO A LA PERSONA NATURAL COMO JURÍDICA**, y es por ello por lo que no debería esperarse efectos mayores para actuar, como así lo demandan los legisladores.

Esta mala redacción ha generado U**N VACIO QUE SERÁ APROVECHADO POR LOS CRIMINALES**, que pueden alegar que nunca cometieron los determinados daños y así, al no encajar en la conducta típica, no habría delito cometido. Y si bien podrían tener la razón, deberíamos preguntarnos qué hacen con la información y la identidad de otra persona si no piensan generar algún daño.

En el caso de Ruth Jeffrey, cuando finalmente se atrapó al acosador, la revelación de su identidad fue tan traumática como el abuso que había sufrido: su ex–novio. Ante esta desagradable experiencia, Ruth Jeffrey ha recibido y sigue recibiendo tratamiento psicológico pues el accionar de su acosar ha generado traumas poderosos y ha destruido por completo su confianza y autoestima[59].

Sin embargo, el caso de Ruth Jeffrey no es el único en el mundo. Existen millones de casos en referencia al delito de robo y/o suplantación de identidad; sin embargo, conociendo antecedentes de este tipo, no se entiende cómo el legislador peruano redacta una norma incongruente y cuyas penas no parecen reflejar la realidad del mundo en el que vivimos.

Las normas que han *preexistido* antes de la Ley N°30096, e incluso las normas actuales, no solo han causado un daño a la población que ha quedado indefensa en materia de ciberdelitos —por no agregar ignorante, ante la poca información y participación que esta ha tenido y sigue teniendo—; sino, además, ha visto **INNECESARIA** considerar a la figura del ciberterrorismo para considerarla delito en nuestro país, o al menos, abrir una puerta de debate.

De acuerdo con las investigaciones realizadas para el presente trabajo de Tesis, la figura del ciberterrorismo no solo es uno de los mayores peligros el día de hoy, sino que guarda una poderosa proyección y cuyo poder será inevitable e imparable si no

[59] Para más información, ver el documental de NatGeo (National Geographic Channel) denominado **«Ciberacoso»** y basado en la experiencia real de Ruth Jeffrey.

empezamos a desarrollar estrategias de ciberseguridad que contemplen su presencia en discusión. Es por ello, incluso jugando en este contexto nuestro pasado, que llama mucho la atención que el legislador peruano no haya incitado a la investigación de este delito existiendo ya estudios y opiniones de organizaciones internacionales como **LA ORGANIZACIÓN DE LAS NACIONES UNIDAS (ONU)** y **LA ORGANIZACIÓN DE ESTADOS AMERICANOS (OEA)**, así como de equipos de inteligencia como es la **CENTRAL INTELLIGENCE AGENCY (CIA)** de los Estados Unidos.

Es deber como peruanos buscar un enfoque correcto en esta legislación que nos permita una protección íntegra contra el peligro que significa la ciberdelincuencia y los principales delitos que esta ejerce; en especial, llevar a mesa de debate la contemplación de la figura del ciberterrorismo como un delito en nuestra legislación.

1.1.2.5. ***Sobre la Ley N°30171 – Modificatoria de la Ley N°30096***

Es a raíz de los errores de la anteriormente comentada Ley N°30096 que el 10 de marzo de 2014 se promulga la Ley N°30171, cuya finalidad era modificar los artículos más controversiales de su antecesora, y los que causaban mayor confusión, como eran los artículos 2°, 3°, 4°, 5°, 7°, 8° y 10°, agregando en muchos casos los términos **«deliberada e ilegítimamente»**, lo que debía significar la aclaración de muchos problemas ante la imposibilidad de detección de los responsables de los delitos, pero que terminó transformándose en un excesivo **«condicionamiento»** de la conducta, generando con ello **NUEVOS VACÍOS LEGALES**. Aprovechados por los delincuentes.

Para comprender con mayor claridad el problema que significó agregar esas dos palabras —ahora condicionantes— es precio volver a analizar el artículo 3°, pero esta vez, de la modificatoria:

> ***Artículo 3° – Atentado a la integridad de datos informáticos***
> *El que deliberada e ilegítimamente daña, introduce, borra, deteriora, altera, suprime o hace inaccesibles datos informáticos, será reprimido con pena privativa de libertad no menor de tres ni mayor de seis años y con ochenta a ciento veinte días multa.*

Visto desde este nuevo punto de vista, con una nueva *supuesta* interpretación, el contenido no ha sido variable. Tal cuál operación matemática, en donde el orden de los factores no altera el producto, la colocación de los términos **«deliberada e ilegítimamente»** abre una nueva puerta con preguntas aún más complicadas para resolver. **«¿Si tengo un ingreso deliberado e ilegítimo, pero no ocasiono daños al sistema, podrán sancionarme bajo esta**

norma?», «¿si mi ingreso no fue ni deliberado ni ilegítimo, pero si causé todo el daño que la norma señala, aún soy objeto de sanción?», «¿Qué pasa si una empresa u organización tiene un problema de DNS que me permite ingresar a su información de manera *casual* solo por encontrarse *libre*, seré objeto se sanción?», «¿esto me obligará a tener equipos de respuestas aún más activos?»

Por si fuera poco, esta misma dinámica siguen los artículos anteriormente mencionados, y en donde las respuestas brindadas por especialistas en seguridad han sido claras. La Ley tiene un foco permisivo para las intromisiones maliciosas, pero es tanta la condición de **«deliberada e ilegítimamente»** que un delincuente puede buscar la manera —y, de hecho, existe— en la que puedan tener acceso a la información, alterarla, y aún tener un ingreso legal. Incluso, puede ser obra de un **INSIDER** —una de las tantas prácticas— que conoce a la perfección las deficiencias de la compañía o sector en el que trabaja, y poder utilizarlas a su favor.

El condicionamiento de la conducta se cumple. Nuevamente, **NADIE ESTÁ OBLIGADO A HACER LO QUE LA LEY NO MANDA NI DEJAR DE HACER LO QUE LA LEY NO PROHÍBE**, pero que sea de conocimiento público que los principales defensores de nuestro derechos en el mundo digital, son los mismo responsables de causar vacíos legales en una de las normas que no solo tenía como finalidad adherirnos al Convenio de Budapest, el más importante en materia del cibercrimen; sino que, además, no han planteado desde su creación una mesa de discusión para ejecutar la mayor cantidad de modificatorias posibles que nos permitan estar seguros —y a las fuerzas del orden hacer su trabajo—, y que han caído en la divulgación de falsedades populistas que aseguran somos un país ciberseguro, cuando nuestra realidad es otra. El Estado aún no aclara quienes son los responsables detrás del manejo de la norma, pero la bandera la sigue ondeando la ONGEI —ahora SEGDI— en cada evento o foro a los que son invitados, pero sin la posibilidad de engañar a los especialistas quienes tienen la total seguridad que, una vez los problemas empeoren, será el mismo Estado quien se lavará las manos.

Una vez más, en el marco de las reuniones para la modificatoria de la Ley N°30096, no se planteó en discusión la necesidad de estudiar y afrontar la figura del ciberterrorismo en nuestra legislación vigente.

1.2. Antecedente II – Ciberterrorismo: Un nuevo horizonte para la criminalidad del terror

1.2.1. *¿Qué es y en qué consiste el ciberterrorismo?*

Durante el desarrollo del *OAS-First Cyber Security Symposium*, llevado a cabo en el año 2016 en Bogotá-CO, Belisario Contreras, director de CICTE-OEA, señaló que, quizás la principal dificultad que se tiene para combatir el terrorismo es que aún no hemos llegado a definirlo como tal, siendo este un delito cuyo concepto varía de acuerdo con el tiempo y la sociedad.

Concuerdo con dicha expresión y la sostengo también para hablar de ciberterrorismo. La practicidad nos demandaría a dar una respuesta rápida y decir que el ciberterrorismo es el terrorismo mismo, pero con temas cibernéticos e Internet. No lejos de la idea, pero sigue siendo primaria. Sin embargo, es esta misma practicidad —y falta de consenso para el concepto único— lo que impide la correcta cooperación internacional, la prevención del delito y castigo de los responsables. Existen muchas definiciones de lo que es terrorismo, y dentro de su contexto mundial ninguna ha sido acogida a nivel universal.

Entendamos entonces primero qué es terrorismo para luego hablar de ciberterrorismo. Para lo mismo, es más dinámico partir de conceptos primarios e ir avanzando a los más complejos y destacados. Si de un concepto básico hablamos, podríamos utilizar el escrito en la *Encyclopedia Britannica*. En sus páginas se defina al terrorismo alegando que **«es el uso sistemático del terror, para coaccionar a sociedades o gobiernos, utilizado por una amplia gama de organizaciones políticas en la promoción de sus objetivos, tanto por partidos políticos nacionalistas y no nacionalistas, de derecha como de izquierda, así como también por corporaciones, grupos religiosos, racistas, colonialistas, independentistas, revolucionarios, conservadores y gobiernos en el poder»**[60].

Los países miembros de la Unión Europea calificaron al delito de terrorismo como **«los actos intencionados que, por su naturaleza o contexto, pueden atentar gravemente contra un país o una organización internacional, intimidar gravemente a una población y obligar indebidamente a los poderes públicos o a una organización internacional a hacer o abstenerse de hacer algo, o a desestabilizar gravemente o destruir las estructuras fundamentales políticas, constitucionales, económicas o sociales»**. Igualmente calificaron a *grupo terrorista* como **«la asociación estructurada de más de dos personas, establecida en el tiempo y que actúa de forma concertada para cometer delitos terroristas»**[61].

[60] Encyclopedia Britannica. Concepto de terrorismo.

[61] SANTIVÁÑEZ MARIN, Juan José M. (2013). **«Seguridad Ciudadana. Estrategias para combatir la Inseguridad Ciudadana»**. Lima, Perú. AFA Editores Importadores S.A. Pp. 103-104. *Citando texto del Diario LA VANGUARDIA en su edición del 07 de diciembre del 2001.*

La ONU conceptualiza al terrorismo como **«la dominación por medio del terror, el control que se busca a partir de actos violentos cuyo fin es infundir miedo»**.
Para CICTE-OEA (2002), el terrorismo **«constituye un grave fenómeno delictivo que preocupa profundamente a todos los Estados Miembros, atenta contra la democracia, impide el goce de los derechos humanos y las libertades fundamentales, amenaza la seguridad de los Estados, desestabilizando y socavando las bases de toda la sociedad, y afecta seriamente el desarrollo económico y social de los Estados de la región»**[62].

Para HIGGINS (1997), reconocida jurista internacional, se entiende que **«'terrorismo' es un término sin significado jurídico. Es simplemente una forma conveniente de aludir a actividades, ya sea de Estados o de individuos, ampliamente desaprobadas y en las cuales los métodos utilizados son ilegales, o los objetos se encuentran protegidos, o ambos»**[63].

El penalista español Miguel Ángel Cano señala que **«lo requerido para que, en rigor, pueda hablarse de delincuencia terroristas en el Derecho Penal Español es la presencia de bandas armadas, organizaciones o grupos que recurran a la violencia o amenaza de la misma contra las personas, provocando con ello alarma o pánico, haciéndolo a su vez de forma organizada con la intención de subvertir el orden constitucional o alterar gravemente la paz pública»**[64].

El Título 22, Sección 2656 (d) del Código de los Estados Unidos, desde 1983, ha utilizado las siguientes definiciones[65]:

- Terrorismo significa una violencia premeditada y motivada políticamente, perpetrada en contra de objetivos no combatientes (la interpretación de no combatientes incluye al personal civil y militar desarmado al momento del incidente) por parte de grupos subnacionales o agentes clandestinos y cuya intención, por lo regular, es influenciar al público.
- Terrorismo Internacional es aquel tipo de terrorismo que involucra a ciudadanos o territorios pertenecientes a más de un país.
- Grupo terrorista abarca todo grupo que practica, o consta de importantes subgrupos que practican el terrorismo internacional.

[62] **CONVENCIÓN INTERAMERICANA CONTRA EL TERRORISMO**. Barbados, 3 de junio de 2002. Documento AG/RES. 1840 (XXXII-O/02). Recuperado del sitio web: http://www.oas.org/xxxiiga/espanol/documentos/docs_esp/agres1840_02.htm
[63] HIGGINS, Rosalyn & FLORY, Maurice (1997). *The general international law of terrorism*. En **«Terrorism and International Law».** Pp. 28. Londres, Inglaterra. Editorial Routledge.
[64] CANO PAÑOS, Miguel Ángel (2013). **«Tratamiento del fenómeno terrorista en el Derecho Penal»**. Lima, Perú. ARA Editores E.I.R.L. Pp. 36-37.
[65] SANTIVÁÑEZ MARIN, Juan José M. **Op. Cit.** Pp. 104. Citando *Departamento de Estado, PATTERNS OF GLOBAL TERRORISM (Patrones de terrorismo mundial). 1993–abril de 1994, IV*.

Otra de las tantas definiciones es la que alberga Manuel Ossorio en su diccionario jurídico. Escribe lo siguiente sobre el delito en mención[66]:

> «*Dominación por el terror (v.). Sucesión de actos de violencia ejecutados para difundir terror. Esta definición tomada del* ***Diccionario de la Academia*** *no tipifica un delito concreto, porque de los actos de* ***terrorismo*** *pueden configurarse otros delitos específicos, ya sea contra las personas, ya sea contra la libertad, contra la propiedad, contra la seguridad común, contra la tranquilidad pública, contra los poderes públicos y el orden constitucional o contra la administración pública. Sin embargo, el terrorismo pudiera estar incluido dentro de los delitos de intimación pública, determinantes de la represión contra quien, para infundir temor público o suscitar tumultos o desórdenes, hiciere señales, diere voces de alarma, amenazare con la comisión de un delito de peligro común o empleare otros medios materiales normalmente idóneos para producir tales efectos; se agrava la pena cuando para ello se emplearen explosivos, agresivos químicos o materiales afines, siempre que el hecho no constituyere delito contra la seguridad pública*».

De este concepto discrepamos un poco en referencia a la **SEGURIDAD PÚBLICA**. Los diferentes intentados realizados por terroristas no solo han causado un caos en la sociedad, sino que a la par han generado estados de inseguridad ciudadana y estados de alerta para con las Naciones. **EL DELITO DE TERRORISMO CONSTITUYE UN PELIGRO PARA LA SEGURIDAD PÚBLICA Y DEL ESTADO**.

De igual modo, siguiendo a Ossorio, se define jurídicamente al **TERRORISTA** como **«defensor o apologista del terrorismo (v.). Autor de delitos encuadrables en esa tipificación del estrago, sin miramiento alguno en cuanto a las víctimas»**[67].

Si de ciberterrorismo hablamos, su conceptualización es variada e histórica. No existe un solo concepto de ciberterrorismo, también guiado por la coyuntura social, política, económica e historia.

En la década de los años 80, se entendió al ciberterrorismo como **«la convergencia del ciberespacio con el terrorismo»**[68]. Para los años 90, **«el ciberterrorismo era el ataque premeditado y políticamente motivado contra información, sistemas, programas y datos**

---

[66] OSSORIO, Manuel (2003). **«Diccionario de Ciencias Jurídicas, Políticas y Sociales»**. 23° Edición actualizada, corregida y aumentada por Guillermo Cabanellas de las Cuevas. Buenos Aires, Argentina. Editorial Heliasta S.R.L.

[67] **Ibid.**

[68] COLLIN, Barry - Institute for Security and Intelligence (1984). **«The future of cyberterrorism: Where the physical and virtual worlds converge»**. 11th Annual international symposium on criminal justice issues. Congreso llevado a cabo en California, EE. UU.

informatizados no combatientes, por parte de grupos terroristas o agentes encubiertos de potencias extranjeras»[69].

Con el paso del tiempo, nuevos conceptos empiezan a matizarse. Es el caso de la explicación que busca dar Dorothy E. Denning, directora del Georgetown Institute for Information Assurance de la Georgetown University, alegando que[70]:

> «*Para calificar como ciberterrorismo, un ataque debe resultar en violencia contra personas o contra la propiedad, o al menos causar el daño suficiente como para generar miedo. Ataques que deriven en muertes o personas heridas, explosiones, colisiones de aviones, contaminación de agua o severas pérdidas económicas pueden ser ejemplos válidos. Serios ataques contra la infraestructura crítica de un país podrían ser actos de ciberterrorismo, dependiendo de su impacto. Los ataques que interrumpen servicios no esenciales o que son básicamente una molestia costosa no entran en esta categoría*».

Para la Dirección general de la policía y la guardia civil - Dirección adjunta operativa jefatura de información del Ministerio del Interior de España (2010), el ciberterrorismo es el **«empleo generalizado de las tecnologías de la información, por parte de grupos terroristas o afines, para la consecución de sus objetivos; utilizando Internet (sistemas informáticos y contenidos) como instrumentos de comisión del delito o como acción del delito»**[71].

El ex oficial de inteligencia naval de los Estados Unidos y periodista especializado en ciberseguridad Dan Verton (2004), asevera que el termino ciberterrorismo es uno de los más incomprendidos, y busca explicarlo diciendo que **«el ciberterrorismo es la ejecución de un ataque sorpresa por parte de un grupo terrorista extranjero subnacional con objetivo político utilizando tecnología informática e Internet para paralizar o desactivar las infraestructuras electrónicas y físicas de una nación, provocando de este modo la pérdida de servicios críticos, como energía eléctrica, sistemas de emergencia telefónica, servicio telefónico, sistemas bancarios, Internet y otros muchos»**[72]. Agrega que el objetivo del ciberterrorismo y sus ataques no solo se centra en impactar

---

[69] POLLITT, Mark - Federal Bureau of Investigation Laboratory (1997). **«CYBERTERRORISM - Fact or Fancy?»**. En National Institute of Standards and Technology, National Computer Security Center. Trabajo presentado en *20th National Information Systems Security Conference*. Pp. 285-289. Baltimore-MD, EE. UU. Proceedings of the 20th National Information Systems Security Conference.

[70] Definición de ciberterrorismo. **«Ciberterrorismo: Una amenaza gubernamental a la privacidad»**. Recuperado de: http://www.paginasprodigy.com/tesisdehackers/cibercap1.html#ciberterrorismo

[71] DIRECCIÓN GENERAL DE LA POLICÍA Y LA GUARDIA CIVIL - DIRECCIÓN ADJUNTA OPERATIVA JEFATURA DE INFORMACIÓN DEL MINISTERIO DEL INTERIOR DE ESPAÑA (2010). **«Sesión tecnológica 6 - Caso de la seguridad en la red: ciberterrorismo»**. En J. RIVERO LAGUNA (Presidencia). XII Congreso DINTEL profesionales IT 2010 TESIC (Tecnologías y Seguridad en Infraestructuras Críticas). Congreso llevado a cabo en Madrid, España.

[72] VERTON, Dan. (2004). En **«Black Ice: La amenaza invisible del terrorismo»**. Pp. 30. Madrid, España. McGraw Hill / Interamericana de España.

en la economía, también en el incremento del impacto de ataques físicos, provocando pánico y confusión en la población.

Germán Vargas Lleras, ex ministro del interior de Colombia (2010), se refirió al ciberterrorismo como **«un fenómeno que evoluciona y varía de acuerdo con las innovaciones de la tecnología y herramientas de la Internet que vuelven vulnerables a los usuarios generando un impacto en un gran conglomerado, que es lo que finalmente pretende el terrorismo»**[73]**.**

Para SANCHEZ DEMERO (2012), el ciberterrorismo supera a la ciberdelincuencia. Señala que ciberterrorismo tiene sus motivaciones en la intimidación, coacción y daño a grupos sociales. actividades delictivas en la red, pero la causa que las motivan y los beneficios que esperan unos y otros son diferentes. Afirma que el ciberterrorismo es **«la evolución que resulta de cambiar las armas, las bombas y los misiles por una computadora para planificar y ejecutar unos ataques que produzcan los mayores daños posibles a la población civil. Esto implica una gran diferencia respecto al cibercrimen: el ciberterrorismo busca originar el mayor daño posible por razones político-religiosas, mientras que las acciones del cibercrimen están dirigidas a conseguir un beneficio principalmente económico»**[74].

La CIA expuso en su famoso GLOBAL TREND 2030 (2013) la mayor de las verdades, dejando en claro que el ciberterrorismo representa una amenaza cada vez mayor no solo para el individuo, sino también para la sociedad en su conjunto, siendo el año 2030 la época de consagración del ciberterrorismo como amenaza global y con poderío absoluto. En sus páginas finales recomienda ir preparándonos para lo que será la mayor amenaza hasta el momento.

Como se puede apreciar, existe una gama que conceptualiza al terrorismo y ciberterrorismo y que varía según el tiempo y las circunstancia. Se ha recurrido a opiniones sobrepasando incluso el tiempo de investigación[75] para demostrar que no existe una constante para conceptualizar esta figura. Es así como, en el proceso de la investigación, se ha desarrollado un concepto propio de ciberterrorismo, el mismo que ya ha sido expuesto en el OAS-First Cyber Security Symposium del 2016 en Bogotá, CO.

---

[73] REDACCIÓN CARACOL RADIO (2010). **«Gobierno anuncia mano dura contra el terrorismo informático»**. 2017, del portal Caracol Radio, sección *Judicial*. Sitio web: http://caracol.com.co/radio/2010/10/10/judicial/1286730420_369451.html

[74] SÁNCHEZ MEDERO, Gema (2012). **«Ciberespacio y el crimen organizado, los nuevos desafíos del siglo XXI»**. Revista Enfoques, Vol. X - N°16, Pp. 74.

[75] Se considera que todo material que se requiere para una investigación no debe tener una antigüedad que supere los cinco años desde la fecha de investigación. Es decir, si no encontramos en el año 2017, nuestra fecha límite para retroalimentarnos en la investigación no debe superar al año 2012; pero al tratarse de un tema tan complejo como el terrorismo y ciberterrorismo, se decidió recurrir a fecha anteriores para demostrar la posición que establece diversos conceptos a lo largo del tiempo que no permiten —todavía— llegar a una idea clara sobre estas figuras.

«*El ciberterrorismo consiste en el uso sistemático del terror e implantación de este a través de Internet y las TIC, los mismos que también son utilizados para captar partidarios al movimiento terrorista, engañar a través de noticias falsas, correos electrónicos, redes sociales y/o acciones diversas, con el fin de desestabilizar a la sociedad*».

Dicho esto, es preciso afirmar que la naturaleza del terrorismo como del ciberterrorismo se encuentra en constante mutación. Es posible que en los próximos años su concepto cambie una vez más, generando nueva investigación y nuevos informes; pero de algo se está seguro, y es que el parámetro destructivo es lo único que se mantiene constante. Es bajo ese punto en que debemos empezar a trabajar tanto en el sector seguridad como en el sector jurídico para encontrar una respuesta o la primera de múltiples respuestas. Si el Derecho llega a comprenderlo, habremos dado un primer paso y, quizás l —bajo apreciación personal—, el más importante de todos.

1.2.1.1. ***Evolución histórica***

Hablar de ciberterrorismo como evolución histórica es hablar de una figura dentro del sistema de Internet. Para muchos especialistas en temas relacionados a Internet y ciberseguridad, y desarrollo de este, nos estaríamos encontrando ante la evolución misma de la figura del terrorismo con dependencia de una conexión al mundo digital y uso de las tecnologías. No obstante, eso no aleja a esta figura de su propia historia dentro de la civilización actual.

Las diversas figuras conceptuales que se han analizado hasta el momento han demostrado que se habla de ciberterrorismo desde la década de los 80s, aceptándolo como esta fusión de la tecnología y el terrorismo, un peligro para la sociedad en crecimiento; y si se recuerda el estudio de la evolución de Internet, es en ese mismo tiempo en que concluye la etapa inicial y se abre la etapa intermedia; en donde se empieza con la globalización de la red de redes y la interconexión; donde aparece el manifiesto hacker y los primeros cimientos del hacktivismo.

El ciberterrorismo es el siguiente paso del terrorismo, es su adaptación —cual virus— al mundo moderno, en una escala más en la pirámide delictiva, más consiente, más poderosa, más intuitiva. La línea temporal de la historia del terrorismo no se ha roto, como algunos quieren creer, una línea que aún se discute donde tiene su primer eslabón, si en el S. I con la organización *Sicari*, en el S. XI con los *Al-Hashshashin* o en el S. XIX con la hermandad *Fenian*, o con cualquier otra organización que posiblemente aún no se haya descubierto.

Lo cierto es que esta vertiente de la historia terrorista daría sus primeros pasos con la aparición de las TIC y sus primeras interconexiones a Internet, al menos desde la base teórica; pues,

como veremos más adelante, su historia operativa —según expertos—, daría inicio a principios del nuevo siglo, en Australia; pero recordemos que ni el mismo terrorismo tiene una época definida. No se descarta que en los próximos años esto pueda cambiar, pero para estos fines utilizaremos la fecha establecida hasta el momento.

1.2.2. *Perfil del ciberterrorista*

1.2.2.1. ***Visión antigua***

La primera figura del ciberterrorista discrepa mucho de la visión actual. Los primeros investigadores resaltaron sus características en los siguientes parámetros:

- Criminal de cuello blanco; es decir, una persona con amplio poder adquisitivo, lo que le permitiría contar con los materiales adecuados para la ejecución de sus crímenes.
- Persona con amplio conocimiento tecnológico y dominio sobre los mismo, pues será quien ejecutará las acciones delictivas.
- Persona guiada por fines políticos y/o religiosos como base para la expansión de su ideología destructiva reflejada en sus ataques.
- El ciberterrorista ataca en organización, por lo que su impulso es mayormente destructivo.
- Tienen un fin u organismo determinado a desestabilizar, concentrando toda su estructura y ataque en ese objetivo

1.2.2.2. ***Visión moderna***

La figura actual del ciberterrorista tiene algunas diferencias con su antecesor, esto debido a que el avance tecnológico ha permitido el desarrollo de otras actitudes y la experiencia ante sus acciones ha permitido un nuevo esquema, que puede llegar a no ser estático, como se ha visto en la historia del terrorismo. Resaltan:

- Persona cuya finalidad es causar pánico o terror a la población, no estando motivado necesariamente por fines políticos, religiosos y/o económicos.
- Persona estratégica y con objetivos claros, no centrando su ataque a un solo esquema; es decir, puede ejecutar múltiples ataques a múltiples organizaciones a la vez.
- Persona con amplio conocimiento tecnológico y de Internet, con dominio sobre los mismos.
- Remarcado resentimiento social, actualmente aprovechado por organizaciones tradicionales para reclutar a expertos en TIC y unirlos a sus filas.

En esta nueva visión se descarta el concepto de criminal de cuello blanco, debido que, con el acceso mayoritario a las TIC e Internet —a diferencia de otras épocas—, es posible conseguir financiamiento de las actividades desde cero. Esto lo dejó en claro Yevgueni Kaspersky, CEO de Kaspersky Lab, quien afirmada en una entrevista para la agencia de noticias EFE (2015) que, **«si cualquier grupo de terroristas del mundo físico decidiera recurrir a servicios de profesionales del cibercrimen, podría hacerlo»**; además, durante su conferencia en Congreso Mundial del Móvil (MWC) de Barcelona (2017) dejó en claro que **«hay muchísimos ingenieros con talento que estarían totalmente dispuestos a realizar este tipo de actos (ciberterrorismo) si están bien pagados, lo cual podría tener consecuencias importantes en los países atacados»**, siendo los ataques a infraestructuras críticas los próximos blancos. Con ello podemos agregar un nuevo punto a la visión moderna: **«un ciberterrorista también puede ser una persona a la que le han pagado para serlo, sin la necesidad que en sus raíces ideológicas brille el causar pánico o terror para tener compatibilidad en los fines»**.

1.2.3. *Partícipes de los efectos de esta figura*

1.2.3.1. ***Sujeto activo: El criminal***

Me atrevo a decir que el Derecho penal —dentro de la academia— pretendería encontrar una visión más profunda de este sujeto activo, algo que vaya más allá de los perfiles anteriormente presentados, pero no dejaría de reconocer que este sujeto activo, dominante de inteligencia bélica y tecnológica, es el pilar que llega a afecta a la sociedad.

No analizamos aquí como sujeto pasivo a una agrupación terrorista, pues quepa la posibilidad que la constitución de una secta terrorista —y especialmente en el mundo digital— llegue a estar constituida por una sola persona con conexión a múltiples servidores y múltiples aparatos tecnológicos, sin limitar sus herramientas a solo computadores y redes públicas. Esta conducta agresiva que configura un tipo de violencia que no necesita contacto corporal para causar daño es el mayor resaltante de este sujeto activo que ––como dice su nombre— mantendrá activo su accionar para que los efectos de la implantación del terror sean constantes y duraderos.

Recordemos que este sujeto activo tiene como principal función desestabilizar a la sociedad, y que para ello se valdrá de todo tipo de medios, como el reclutamiento de nuevos miembros a sus equipos, los que se encontraran en cualquier parte del globo; o la invasión a medios y sistemas, demostrando que pueden estar presente en donde exista una conexión a Internet.

1.2.3.2. ***Sujeto pasivo: La sociedad***

Tal cual expresa el título, la sociedad en la que vivimos, compuesta por lo tangible y lo digital, es la mayor afectada ante la figura del ciberterrorismo, capaz de desestabilizar desde la estructura económica como la cultural, todas interconectadas al quinto poder. El Perú aún no es consciente de la proyección que trae consigo el ciberterrorismo, y así ha quedado en claro con lo redactado hasta este momento.

Internet y las TIC han desestabilizado las barreras que los movimientos migratorios aún mantienen para colocar a una persona en un foco determinado del globo —y sin siquiera moverse se sus asientos o países—. No existe barreras de transporte con estos componentes, ni menos límites de ingenio. Si podemos comprender dos de los conceptos más simples de Internet —la Gobernanza de Internet trae conceptos más complejos—, ¿por qué es difícil comprender para nuestros legisladores o responsables de SEGDI u otras instituciones sobre la peligrosidad que representa una figura como el ciberterrorismo?

Repito, la sociedad ya no es solo física, y pensar que la amenaza terrorista solo pisará suela nacional de manera tangible y que solo de esa manera actuaremos, es no ver más allá de la realidad que ya otros países en la región vienen discutiendo. Repito, un desequilibrio en la sociedad como puede generar una figura tal como el ciberterrorismo no solo crea una vertiente de inseguridad equiparable —o mayor— a la que se vive actualmente en el país; además de genera **PROBLEMAS ECONÓMICOS, POLÍTICOS Y SOCIALES**, que destruirían la poca estabilidad que nos queda como nación.

1.2.3.3. ***Bien Jurídico Protegido: La seguridad de la sociedad***

Con relación al **BIEN JURÍDICO PROTEGIDO** no hay mayor vulnerabilidad que la que se vive en el estado de seguridad de nuestra nación. Como hemos comprendido durante el desarrollo de esta tesis, la misma que expone conductas y perfiles, un ciberterrorismo busca implantar el terror en la sociedad y desestabilizarla en todos sus pilares, utilizando para ello el medio de comunicación universal por excelencia, y es Internet.
Detener sus exposición en la red de redes es un trabajo que demanda mucho tiempo y dedicación, especialmente por la complejidad normativa que envuelve —por ejemplo— una simple publicación en Internet, pero hay que recordar que en ello radica la responsabilidad del Estado, acentuando en la no prohibición de contenido, sino en la respuesta ante este contenido que llega a afectar a la sociedad y su seguridad, sin contar aún los ataques a

través de tecnologías y medios digitales que estos individuos puedan ocasionar.

Según la Constitución Política del Perú, en su Artículo 163°, señala[76]:

> «*El Estado garantiza la seguridad de la Nación mediante el Sistema de Defensa Nacional.*
> *La Defensa Nacional es integral y permanente. Se desarrolla en los ámbitos interno y externo. Toda persona, natural o jurídica, está obligada a participar en la Defensa Nacional, de conformidad con la ley*».

Debemos contemplar que la protección de nuestra integridad en la actual sociedad que se encuentra dividida en tangible y digital recae en manos de las fuerzas armadas nacionales, conformadas por ejército, marina y fuera aérea; la que, ante la complejidad de temas ciber —y a criterio de quien escribe— deben trabajar de la mano con la PNP. Si bien las discusiones en materia de ciberseguridad se vienen tratando en este último año, ninguna de ellas ha puesto sobre la mesa la necesidad de debatir sobre la figura del ciberterrorismo como un delito creciente y presente, aun habiendo estado presente la discusión sobre las nuevas funciones de la DINI como responsable de la ciberseguridad nacional. Si bien no es función de estas fuerzas promulgar leyes, su experticia si debía hacerse presente como nuevo detonante para poner sobre la mesa la discusión sobre la figura del ciberterrorismo, pero desconozco el porqué de la resistencia.

Si el bien jurídico protegido se ve afectado por la inestabilidad de la seguridad estatal, también se verán afectados otros componentes como el crecimiento económico y social del país. Ello traería consigo estragos de hace más de una década, en donde el miedo y la inseguridad primaban y obligaban a muchos compatriotas a migrar del país o a enterrar a sus familiares y/o identificarlos entre los escombros de algún edificio efecto de un coche bomba. Dado que en aquel entonces vivíamos un problema de inflación económica, el terrorismo de aquel tiempo solo terminó por empeorar las cosas. El terrorismo de este tiempo tiene campos aún mayores en donde una inflación o una migración no son impedimento para seguir en el proceso de implantación del terror. Debemos comprender que el ciberterrorismo no tiene límites, y que el daño que puede hacerle a la seguridad de la nación, a este bien jurídico protegido, puede tener daños irreparables o que cuesten reparar solo con el tiempo y la inversión. La prevención es la fórmula actual ante esta figura, y es por ello por lo que deberíamos preguntarnos qué tanto hace el Estado para salvaguardar la protección de este bien tan preciado.

[76] **Seguridad de la Nación**. Artículo 163° de la Constitución Política del Perú. Año 1993.

1.3. Vertientes principales del ciberterrorismo con la utilización de Internet y la tecnología

Característico de los movimientos terroristas siempre ha sido su manera de actuar. Aunque guardan muchos parámetros comunes ante la implantación del terror, cada movimiento bélico ha guardado un sello característico durante su presencia en ciertas etapas. De la misma manera, la figura del ciberterrorismo tiene maneras de actuar, no siendo la destrucción para lo único en lo que empeñan el uso de TIC e Internet.

1.3.1. *Como apología del terrorismo*

Antes de explicar el uso de la apología por parte del ciberterrorismo, debemos de entender qué es apología y por qué debemos considerarla como parte de su estrategia. El Diccionario de la Real Academia Española de la Lengua lo define como **«discurso de palabra o por escrito, en defensa o alabanza de alguien o algo»**.

Ante lo expuesto podemos deducir que hacer *apología de algo* no necesariamente es un delito, más bien expresa el sentir o pensar sobre un determinado personaje, lanzando pompas de sus hazañas que enaltezcan su carácter. Por ejemplo, se podría hacer *apología* de un personaje histórico como un héroe nacional (Ej. Miguel Grau); podría ensalzarse sus grandes obras y su patriotismo, su caballerosidad en el combate y su aguerrido espíritu para defender a su patria, pero no por ello se ha cometiendo *delito de apología* como se encuentra tipificado en el código penal peruano vigente. Caso contrario, aquellos que realzan *valores* en criminales —y entiéndanse valores como término sarcástico que señalan actos en contra de los valores e integridad humana— para incitar a la población a fines criminales o alterar parte de la historia nacional para confundir a determinado sector social, si estarían considerado como *delito de apología*.

Cuando se combina el empleo de la apología con el poder de Internet, a lo que realmente nos enfrentamos es a encontrar la ilegalidad —si es que existe— en las expresiones que pueda verter la persona sobre determinado persona o contenido. Esto se debe a que uno de los principios más importantes que existen para Internet —y que defiende fielmente la Gobernanza de Internet y organismos internacionales— es la libertad de expresión; pero se debe reconocer cuando empieza y cuando finaliza la libertad de expresión de una persona, sin afán de ser autoritario o cero democrático, sino en afán de protección de la sociedad y de los individuos, pues toda libertad de expresión llega a su fin si es que, en este ejercicio, se afectan derechos fundamentales de otra persona, o en este caso, lo derechos fundamentales de la sociedad.

Para comprender mejor la figura delictiva de la apología, debemos remontarnos al código penal peruano en todas las circunstancias

temporales. En primera instancia, el código tipificaba la apología de la siguiente manera

> ***Artículo 316°: Apología***
> *El que, públicamente, hace la apología de un delito o de la persona que haya sido condenada como su autor o partícipe, será reprimido con pena privativa de libertad no menor de uno ni mayor de cuatro años.*
>
> *Si la apología se hace de delito contra la seguridad y tranquilidad públicas, contra el Estado y la defensa nacional, o contra los Poderes del Estado y el orden constitucional, la pena será no menor de cuatro ni mayor de seis años.*
>
> *Si la apología se hace del delito de terrorismo o de la persona que haya sido condenada como su autor o partícipe, la pena será no menor de seis ni mayor de doce años. Además, se le impondrá el máximo de la pena de multa previsto en el artículo 42 e inhabilitación conforme a los incisos 2, 4, y 8 del artículo 36 del Código Penal*[77].

Luego de que el artículo 2° del Decreto Legislativo N°982, publicado el 22 julio 2007 modificara el artículo, el actual código penal peruano hace referencia al delito de apología de la siguiente manera:

> ***Artículo 316°: Apología***
> *El que públicamente hace la apología de un delito o de la persona que haya sido condenada como su autor o partícipe, será reprimido con pena privativa de libertad no menor de uno ni mayor de cuatro años.*
>
> 1) *Si la apología se hace de delito previsto en los artículos 152° al 153°-A, 200°, 273° al 279°-D, 296° al 298°, 315°, 317°, 318- A, 325° al 333°; 346° al 350° o en la Ley N°27765, Ley Penal contra el Lavado de Activos o de la persona que haya sido condenada como su autor o partícipe, la pena será no menor de cuatro ni mayor de seis años, doscientos cincuenta días multa, e inhabilitación conforme a los incisos 2,4 y 8 del artículo 36° del Código Penal.*
>
> 2) *Si la apología se hace de delito de terrorismo o de la persona que haya sido condenada como su autor o partícipe, la pena será no menor de seis ni mayor de doce años. Si se realiza a través de medios de comunicación social o mediante el uso de tecnologías de la información y comunicaciones, como Internet u otros análogos, la pena será no menor de ocho ni mayor de quince años; imponiéndose trescientos sesenta días multa e inhabilitación conforme a los incisos 2, 4 y 8 del artículo 36° del Código Penal.*

Ambos artículos hacen referencia al terrorismo en su segundo párrafo, pero es gracias a la modificatoria del 2007 que empieza a tomarse en cuenta a la divulgación por uso de las TIC e Internet. Sin embargo, para junio de

[77] Párrafo incorporado por el Artículo Primero del Decreto Legislativo N°924, publicado el 20-02-2003.

2017, a raíz del proyecto de Ley N°1395/2016-CR, se aprobaría una última modificatoria generando así el artículo 136°-A, dando paso a una doble figura —debatible si es necesaria— y a dos artículos: uno para el delito de apología y otro para el delito de apología del terrorismo. Los nuevos artículos se enmarcan de esta manera.

Artículo 316°: Apología

El que públicamente exalta, justifica o enaltece un delito o a la persona condenada por sentencia firme como autor o partícipe, será reprimido con pena privativa de libertad no menor de un año ni mayor de cuatro años.

Si la exaltación, justificación o enaltecimiento se hace de delito previsto en los artículos 152 al 153-A, 200, 273 al 279-D, 296 al 298, 315, 317, 318-A, 325 al 333, 346 al 350 o de los delitos de lavado de activos, o de la persona que haya sido condenada por sentencia firme como autor o partícipe, la pena será no menor de cuatro ni mayor de seis años, doscientos cincuenta días de multa, e inhabilitación a los incisos 2, 4 y 8 del artículo 36 del Código Penal.

Artículo 316°-A: Apología del terrorismo

Si la exaltación, justificación o enaltecimiento se hace del delito de terrorismo o de cualquiera de sus tipos, o de la persona que haya sido condenada por sentencia firme como autor o partícipe, la pena será no menor de cuatro años ni mayor de ocho años, trecientos días multa e inhabilitación conforme a los incisos 2, 4, 6 y 8 del artículo 36 del Código Penal.

Si la exaltación, justificación o enaltecimiento del terrorismo se realiza: a) en ejercicio de la condición de autoridad, docente o personal administrativo de una institución educativa, o b) utilizando o facilitando la presencia de menores de edad, la pena será no menor de seis años ni mayor de diez años e inhabilitación, conforme a los incisos 1, 2, 4 y 9 del artículo 36 del Código Penal.

Si la exaltación, justificación o enaltecimiento se propaga mediante objetos, libros, escritos, imágenes visuales o audios, o se realiza a través de imprenta, radiodifusión u otros medios de comunicación social o mediante el uso de tecnologías de la información o comunicación, del delito de terrorismo o de la persona que haya sido condenada por sentencia firme como autor o partícipe de actos de terrorismo, la pena será no menor de ocho años ni mayor de quince años e inhabilitación, conforme a los incisos 1, 2, 4 y 9 del artículo 36 del Código Penal."

El círculo cierra con la presencia de una Ley que ha sido catalogada por algunos como **«Ley mordaza»** y, por otros, como una ley inconstitucional, al prohibir siquiera la libertad de expresión; pero regresamos al primero

punto en dónde se cuestionaba la libertad de expresión, y en donde iniciaba y finalizaba ese derecho. Pronunciarse a favor de un terrorista **NO CONSTITUYE LIBERTAD DE EXPRESIÓN**, y no podemos disfrazar ese actuar con un derecho tan peleado por muchos países como la libertad de expresión.

Lo que es de aplaudir es que en dos de las tres líneas temporales en las que existe el delito de apología se toma en cuenta a las TIC e Internet como un medio de propagación; no obstante, la práctica no es meritoria. Son muchas las páginas con contenido, desde blogs hasta redes sociales que han sido invadidas por grupo terroristas tradicionales como Sendero Luminoso (SL) y el Movimiento Revolucionario Tupac Amaru (MRTA); así como sus nuevas vertientes tales como el Movimiento por la Amnistía y Derechos Fundamentales (MOVADEF) y, su nuevo rostro, el Frente de Unidad y Defensa del Pueblo Peruano (FUDEPP), ambas organizaciones sostenidas por jóvenes que desconocen la realidad del Perú y que son fácilmente manipulables. Debemos aceptar también que la modificatoria del artículo 316° se debió al debate generado luego de las marchas de abril y mayo de 2017 organizadas por MOVADEF, en donde se utilizaron pancartas con imágenes de Abimael Guzmán y mensajes con contenido delictivo de acuerdo con la normativa vigente[78], y no tuvo como base la comunicación que vienen teniendo estas organizaciones a través de Internet y las redes sociales para tener más poder en base a la juventud.

Es posible encontrar contenido web que demuestra esta afirmación. Páginas como Sol Rojo (http://www.solrojo.org/) tiene un contenido que entremezcla pensamientos de izquierda con la apología del terrorismo a través de alabanzas y justificaciones a las acciones de Abimael Guzmán; o como ¡Abajo la farsa de juicio! (https://abajolafarsadejuicio.blogspot.pe/), blog con contenido que busca limpiar la imagen de Abimael Guzmán y desinformar a la población con una apología del terrorismo disfrazada de justificaciones absurdas. FUDEPP tiene dada de baja su página web (http://fudepperu.blogspot.pe/), pero eso no le impidió mudarse a una plataforma más llamativa para la juventud como Facebook (https://www.facebook.com/fudeppperu/) donde continúan su disfrazada campaña política e imágenes que reafirman el delito de apología.

El terrorismo tradicional —tal cual se explicó líneas arriba— ha dado un paso más en su evolución y va perfeccionando su plan de adaptación para con los jóvenes. Han encontrado en la cultura un punto clave para la expansión de su ideología, como lo estipulara Abimael Guzmán en su **«Plan Amanecer»**. Han entendido el poder que tiene Internet y los medios de comunicación que ahí se albergan, lo que les está permitiendo tener un mayor alcance de su verdadero potencial. Han aprovechado vacíos anteriores en las normas para el ejercicio de su afán delictivo; y no será sorpresivo que pronto encuentren los nuevos vacíos. Quizás, esta vez, utilicen la pancarta de la libertad de expresión, lo que debe evitarse a toda

[78] Cfr. PIGHI BEL, Pierina (2017) **«Qué es el Movadef, la polémica organización que vinculan con Sendero Luminoso en Perú y a la que acusan de apología al terrorismo»**. Del portal digital BBC Mundo. Sitio web: https://www.bbc.com/mundo/noticias-america-latina-40856626

costa. Este tipo de acciones ya han sido utilizadas por ISIS desde hace un par de años, a través de distribución de vídeos donde realizaban ejecuciones hasta audios y documentos distribuidos en múltiples idiomas con el contenido de su ideología. Sí, Internet alberga el ciberterrorismo en la cuestión de apología, pero estamos hablando de la web superficial, y es en esa web en la que se ha sustentado nuestra normativa vigente. Nos queda por explorar la Deep web y Dark web para determinar si también hay presencia ciberterrorista nacional, porque la internacional ya existe y es igual de peligrosa.

1.3.2. *Como medio de implantación del terror*

El ciberterrorismo —como figura— y los ciberterroristas —como actores o participes— entiende el poder de Internet y los medios que se complementan, encontrando en este hábitat un lugar que se ajusta a sus planes de expansión de implantación del terror, especialmente porque Internet no tiene límites, y porque muchas veces las legislaciones internacionales han fallado en los sistemas de regulación de conductas que se producen en este continente de información.

Durante los primeros años de esta investigación, se profundizo en buscar grupos terroristas conocidos en el ambiente digital, para tener una idea de cuántos de ellos habían decidido expandir su accionar en el ciberespacio, o si podría llamárseles grupos ciberterroristas en un futuro no tan lejano. Es así que se llegó a las páginas anteriormente expuestas, así como a mucho contenido en redes sociales —algunos ya no están vigentes— en donde se exponían ideas, se citaban a reuniones o se publicaban imágenes cruentas que reflejaban parte de la historia vivida entre la década de los 80s y 90s; perfiles en donde se justificaban el accionar terrorista y se incentivaban unirse a sus filas acompañados de falsas notas para invitar a jóvenes a conocer el movimiento y sus *beneficios*, sabiendo que estos, por la edad y la ignorancia —así como el no haber vivido en la época del terror ni haber recibido información precisa sobre los hechos— son presa fácil de sus manipulación.

Atrás quedaron las imágenes que SL publicara alguna vez por el 2014, cuando aún existía el perfil de Facebook y parecía que los filtros no eran efectivos; imágenes que traía a la memoria aquella época de nuestra historia republicana marcada de dolor y pesadilla, en donde se mataba a gente inocente, policías, niños, adultos, ancianos, y a los traidores de su movimiento, quienes eran torturados y luego colgados con una soga al cuello en alguna calle o plaza de la capital, acompañados con un explícito cartel con la frase **«así mueren los perros traidores»**. Niños portando armas con miradas frías y decididas, cadáveres de personas en la escena más explícita cubiertos de sangre y reposando sobre el pavimento, pronunciamientos dando vivas por el regreso del movimiento y exigiendo libertades de sus camaradas apelando a una reconciliación que no tiene pies ni cabeza, todo ello en un ecosistema imparcial como lo es Internet y que haría pensar que se trata de una mente que no comprende el

sufrimiento de una época, pero que en realidad se trata de ellos, de camaradas de SL que actúan por medio del canal que contacta directamente con la mente y el corazón de los jóvenes, su mayor presa.

Sin embargo, no todo accionar del ciberterrorismo se define en recuerdo de una era terrorífica; sino también, en factores que llegan a convertirse en psicosociales que implantan un terror tal que la búsqueda de la verdad o la comprobación de lo que se diga para demostrar su veracidad queda en segundo plano, haciendo que cualquier noticia sea tomada como cierta, cuando debería pasar por un previo filtro. Estas noticias falsas —conocidas también como *fake news*—buscan que su terror se convierta en un terror a gran escala. Sino recordemos el caso de los JUGOS PULP®[79] en el año 2006, en donde un correo viral decía a pie lo siguiente[80]:

> *Asunto: PARA TENER EN CUENTA REFRESCO PULP CON SIDA*
> *Contenido del correo:*
> *YO NO SE SI ES CIERTO, PERO POR SI ACASO. :)*
> *PARA TENER EN CUENTA REFRESCO PULP CON SIDA.*
> *POR FAVOR TOMENLO EN SERIO¡¡¡¡¡¡¡EL DIA DE AYER POR LAS NOTICIAS SALIO EL REPORTAJE DE UN EMPLEADO DE LA FABRICA DE JUGOS PULP QUE RESENTIDO POR LOS TRATOS DE SUS ADMINISTRADORES POR EL HECHO DE SER UNA PERSONA CON VIH SE CORTO LAS VENAS Y VERTIO SU SANGRE EN LOS TANQUES DONDE SE ENCUENTRA EL PRODUCTO. ESTO ES VERIDICO ASI QUE A LOS ADICTOS A ESTE REFRESCO TAN DELICIOSO POR UN BUEN TIEMPO Y REPETIMOS POR UN BUEN TIEMPO SE ABSTENGAN DE CONSUMIR ESTA BEBIDA "PULP" ..POR FAVOR REENVIEN ESTE MENSAJE A TODAS LAS PERSONAS QUE CONOSCAN Y QUE APRECIEN".*

Para algunos, este mensaje no pasó a ser una de las tantas cadenas con fines SPAM. Para otros —la gran mayoría— fue aceptado como referencia de una realidad tan preocupante y como noticia verdadera, tomando precauciones para cuidar a los suyos. Este mismo mensaje fue trasmitido en los principales noticieros de la época como un informe verídico. Lo cierto es que este mensaje distribuido por correo electrónico tenía dos finalidades principales, siendo la primera la *implantación del terror y manipulación psicológica*; y la segunda, *la obtención de correos electrónicos para el resguardo de base de datos*. Sin embargo, también existió una finalidad secundaria —algunos dirán que también puede considerársele como principal— y es la de *sabotear el producto y la empresa distribuidora*. Lo único veraz alrededor de este mensaje es que se trata de un clásico ejemplo de ciberterrorismo y metodologías de implantación del terror, un método que emplea *fake news* para generar

[79] Marca registrada. N° de CertificadoP00140496.

[80] Copia del correo cadena extraído de **YAHOO! GRUPOS – ESPAÑA**. Publicado el 24 de noviembre de 2006. Recuperado de: http://es.groups.yahoo.com/group/Juanalarquinas/message/142

desconfianza en la población —en este caso, desconfianza hacia el consumidor—, efecto que no tiene un tiempo establecido de duración[81].

Los hechos que se dieron después demostraron el poder de la viralización de este tipo de notas. La empresa se encargó de desmentir dicha noticia ––que siquiera nunca fue comprobada por los principales medios—, pero la desconfianza de las personas era más latente, por lo que no era de extrañar que algunas tiendas retiraran el producto por un tiempo de sus anaqueles. Y sí, las noticias en Internet tienen un nivel de propagación más alto que las noticias proyectadas en medios tradicionales como la prensa radial, escrita y televisiva, y más si la población *millennial* y *centennial* se ha incrementado en los últimos años —y sigue en aumento—. Una noticia de este tipo puede ser fácilmente reconocida; pero una noticia bien maquinada y con los parámetros muy bien cuidados —entre ellos, la ortografía— puede impactar a la sociedad de manera más rápida y eficaz.

Entonces, son dos tipos de publicaciones —hasta el momento— que pueden ser ejercidas por ciberterroristas o por personas que ejecutan actividades ciberterroristas: las *fake news* y el contenido de imágenes de archivo, en donde estas últimas pueden incluso ser confundidas con material visual para estudios académicos. Lo cierto es que estos últimos van acompañados por frases que incitan al miedo. La fusión de ambas puede llegar a tener un gran impacto en la sociedad y hacer el trabajo más difícil en una época en la que ya debemos cuestionarnos todo aquello que habita en Internet.

En 2015, investigadores de la Universidad de Alabama en Birmingham descubrieron que la verificación automatizada y humana para los sistemas de autenticación de usuarios basados en voz son vulnerables a los ataques de suplantación de voz. Este trabajo fue presentado en el *20th European Symposium on Research in Computer Security* realizado en Viena, Austria; donde explicaron que con unos minutos de audio de la voz de una víctima —transmitidos en vivo o desde videos o programas de radio, de YouTube o llamadas SPAM—, un atacante puede crear una voz sintetizada que puede engañar a los humanos y a los sistemas de seguridad biométricos de voz utilizados por algunos bancos y teléfonos inteligentes; incluso puede hablar por un micrófono y el software lo convertirá para que las palabras suenen como si la víctima las hubiera hablado[82][83].

[81] En el caso de PULP® y el correo del 2006, el impacto fue tal que pasó un tiempo para que las personas volvieran a consumir un producto de la compañía.

[82] Cfr. STEPHEN, Katherine (2015) **«UAB research finds automated voice imitation can fool humans and machines»**. 2017, de UAB News - The University of Alabama at Birmingham. Sitio web: http://www.uab.edu/news/research/item/6532-uab-research-finds-automated-voice-imitation-can-fool-humans-and-machines

[83] Cfr. SOLON, Olivia (2017) **«The future of fake news: don't believe everything you read, see or hear»**. 2017, del portal web The Guardian, sección *Tecnologías*. Sitio web: https://www.theguardian.com/technology/2017/jul/26/fake-news-obama-video-trump-face2face-doctored-content

Otro claro ejemplo es el proyecto *Synthesizing Obama*[84] de la Universidad de Washington, donde tomaron el audio de uno de los discursos de Obama y lo usaron para animar su rostro en un video completamente diferente con una precisión increíble —gracias a la formación de una red neuronal recurrente con horas de metraje—, para tener una idea de cuán insidiosas pueden ser estas adulteraciones[85].

La tecnología de investigación ha puesto al descubierto dos modalidades que ya son utilizadas en las *fake news*, y que no se descarta puedan ser utilizadas por el ciberterrorismo en un futuro. Recordemos que en ambas investigaciones ya se habla de malos usos, ataques y víctimas, y pueda ser posible que el mal uso en potencia es solo cuestión de tiempo. Pero, regresando a los medios de implantación del terror, no todas las notas que se publican son *fake news*, tal es el caso de los vídeos que en 2014 ISIS empezara a divulgar como parte de su campaña de terror y represalia a los EE. UU. por su intervención en Medio Oriente, en donde decapitaban a ciudadanos de este país como el trabajador humanitario Peter Kassig[86] y los periodistas Steven Sotloff[87] y James Foley[88]. Ese mismo año también difundió un vídeo y e imágenes explícitas de la decapitación de 18 soldados sirios[89]; y en agosto de 2017 publicó dos videos, uno amenazando a Donald Trump, actual presidente de los EE. UU., y en otro prometiendo más ataques a España on que si este no se retira de la coalición internacional, que lidera EE. UU. y que lucha contra el yihadismo en Siria e Irak[90].

El terrorismo tradicional se expande hacia métodos ciberterroristas. ISIS es el ejemplo más actual, pero eso no deslinda que grupo como SL y MRTA no empiecen su movimiento, siendo el primero de ello —por el momento— el más activo y el más peligroso en nuestro país. Las páginas web y las redes sociales pasan a ser su primer filtro de contenido, pero que no sorprenda que en un futuro sus metodologías cambien. Por la década de los 80s y 90s era el **«Pensamiento Gonzalo»**, la ideología que dictaba el

---

[84] Cfr. SUWAJANAKORN, Supasorn; SEITZ, Steven M. & KEMELMACHER-SHLIZERMAN, Ira (2017) **«Synthesizing Obama: Learning Lip Sync from Audio SIGGRAPH 2017»**. 2017, de GRAIL: Graphics and Imaging Laboratory of the University of Washington's. Sitio web: http://grail.cs.washington.edu/projects/AudioToObama/

[85] SOLO, Olivia (2017). **Óp. Cit.**

[86] Cfr. REDACCIÓN UNIVISIÓN (2014). **«ISIS difundió el video de la decapitación del estadounidense Peter Kassig»**. Del portal Univisión Noticias. Sitio web: http://www.univision.com/noticias/noticias-del-mundo/isis-difundio-el-video-de-la-decapitacion-del-estadounidense-peter-kassig

[87] Cfr. REDACCIÓN INFOBAE (2014). **«Video: así decapitó el ISIS al periodista estadounidense Steven Sotloff»**. Del portal Infobae, sección *Política*. Sitio web: https://www.infobae.com/2014/09/02/1592006-video-asi-decapito-el-isis-al-periodista-estadounidense-steven-sotloff/

[88] Cfr. CARTER, Chelsea J. (2014). **«Video shows ISIS beheading U.S. journalist James Foley»**. Del portal CNN. Sitio web: http://edition.cnn.com/2014/08/19/world/meast/isis-james-foley/index.html

[89] REDACCIÓN INFOBAE (2014). **«El Estado Islámico se radicaliza y difunde en video su ejecución más salvaje»**. Del portal Infobae, sección *Política*. Sitio web: https://www.infobae.com/2014/11/17/1609281-el-estado-islamico-se-radicaliza-y-difunde-video-su-ejecucion-mas-salvaje/

[90] REDACCIÓN INFOBAE (2017). **«El Estado Islámico publicó dos videos: en uno utiliza a un niño para amenazar a Trump y en otro promete más ataques a España»**. Del portal Infobae, sección *Mundo*. Sitio web: https://www.infobae.com/america/mundo/2017/08/23/el-estado-islamico-publico-dos-videos-en-uno-utiliza-a-un-nino-para-amenazar-a-trump-y-en-otro-promete-mas-ataques-a-espana/

levantamiento armado y la destrucción de los cimientos de la sociedad peruana para levantar algo nuevo, sin importar la vida de inocentes. En este tiempo es el **«Plan Amanecer»**, en donde buscan la expansión de su ideología a través de participación política y cultura, siendo las nuevas víctimas los jóvenes desconocedores de la cruenta realidad vivida el siglo pasado y nos catapultó como la era más sangrienta de nuestra historia republicana y uno de los países que albergó a uno de los más grandes genocidas de todos los tiempos.

1.3.3. *Como arma de ataque contra la sociedad*

Si la apología y la implantación del terror no fueran suficiente, el empleo de las TIC para efectuar ciberataques es una práctica común que —podría decirse— existe desde las máquinas aparecieron, y que se perfeccionaron con Internet. Hablamos de hardware y software avanzado, no del típico sistema de oficina —que también podría ser utilizado para una amenaza INSIDER, pero no es el caso—, que en otra vertiente también generó la ciberguerra.

Los ciberterroristas utilizan estos medios para realizar ataques más rápido y sin intervención humana presencial, lo que no restaría cuerpos a su movimiento; pero lo más importante, es que les permite ejecutar ataques sin la necesidad de moverse de su campo de ejercicio. Un ejemplo sería un ataque al sistema de seguridad del Ministerio del Interior de Perú que se realizó desde una oficina en Turquía. El empleo de BOTNETS es otra alternativa que permita un ciberataque simultáneo a múltiples sistemas ubicados en el globo y que no estén necesariamente interconectados.

Con la dependencia tecnológica, y la mala experiencia en ciberseguridad de muchos países de la región —especialmente, el nuestro—, podríamos tentar una lista de posibles objetivos que tenga en mente una organización ciberterrorista o un grupo terrorista que realiza actividades de este tipo:

- Colapso de redes telefónicas, de comunicaciones, de sistemas bancarios y sustracción de dinero de las cuentas.
- Ataques contra sistemas militares aéreos, marítimos y terrestres.
- Sabotajes al sistema de seguridad y control de aeropuertos, terrapuertos y puertos marítimos, con intervención en el tráfico de estos.
- Sabotajes a empresas, entidades del estado, centrales hidroeléctricas y de servicios básicos.
- Destrucción de bases de datos estatales y particulares, así como de sus sistemas de ciberseguridad.
- Lanzamiento de bombas o reprogramación de objetivos.
- Ciberataques en cadena y con múltiples objetivos con empleo de malware de todo tipo tales como virus, troyanos, ransomwares, entre otros.

Como veremos líneas más adelante, ya existen antecedentes de este tipo de accionar, en donde no necesariamente se han empleado ataques a distancia o el hardware o software más avanzado, pero si la capacidad y conocimiento para sobre lo sistemas a los cuales se buscaba vulnerar. El campo de la ciberseguridad, así como el de los ciberataques, es muy amplio y evolutivo. Lo que podemos usar como sistema defensivo el día de hoy pueda ser inservible en menos de una hora. Nunca un ataque es igual a otro, y esa es la primera premisa que debemos entender. Nuestros legisladores han cometida ese error muchas veces cuando de ciberdelitos se trata, creyendo que por existir la presencia de una máquina siempre será la misma acción y por ello las normas deben ser estáticas; olvidando que detrás de esos sistemas hay un humano que piensa y no comete el mismo error dos veces seguidas.

1.3.4. *Como medio de captación*

En resumidas palabras lo hemos visto con el delito de apología y los métodos que utilizan para captar adolescentes por medio de webs y redes sociales. La información publicada se propagan cada segundo y los jóvenes tienen acceso a ello con mayor facilidad. En nuestro país, hasta donde se conoce, la captación por parte de grupo terroristas que ejercen acciones ciberterroristas han sido con fines políticos y de alteración de histórica. Esto no quiere decir que sea menos peligros que aquel que realiza un ataque desde un computador o sistema electrónico, pues como dijera Abimael Guzmán la noche del 12 de setiembre de 1992, día glorioso de su captura, **«el cuerpo muere, pero las ideas quedan»**. Cuanta razón expresaba tan terrorífico mensaje y que hoy se ve reflejado en jóvenes que no entienden bien las despiadadas ideas; pero al fin de cuentas, él está en la cárcel y las ideas en la calle.

La capacidad de captación ha variado con el paso del tiempo. A mediados de los años 80, *Al Qaeda* comenzó a hacer su propaganda —y en especial, la de Bin Laden— a través de una revista mensual *Al Jihad*; pero, con la generalización del uso de Internet, comenzaron con la publicación de su periódico en inglés Inspire, dirigido especialmente a los jóvenes yihadistas[91]. En 2007, desde el Ministerio del Interior saudí se afirmaba que el 80% de todos los jóvenes saudíes que habían sido reclutados por los yihadistas en su país, lo habían sido utilizando internet[92]. En 2015, Javier Nistal Burón, subdirector general de tratamiento y gestión penitenciaria del Ministerio del Interior de España, informó en una entrevista que el 80% de la captación y adoctrinamiento de nuevos miembros por parte del terrorismo yihadista se da en las redes sociales e internet[93]. En 2016,

[91] GUTIÉRREZ, Angélica (2012). **«Cómo el terrorismo islamista usa Internet»**. Quadernos de criminología: revista de criminología y ciencias forenses, N°19, Pp. 9. 2017, de DIALNET Base de datos.

[92] **Ibid.** Pp. 11

[93] REDACCIÓN EFE. MELILLA/ LOGROÑO (2015). **«El 80% del adoctrinamiento yihadista se produce por internet»**. 2017, de El Heraldo. Sitio web: http://www.heraldo.es/noticias/nacional/2015/07/23/el_del_adoctrinamiento_yihadista_produce_internet_405374_305.html

Francisco Hernández Guerrero, fiscal de criminalidad informática de Granada, afirmó que la captación con fines terroristas es un riesgo latente de la sociedad que preocupa a las fuerzas y cuerpos de seguridad y a la administración de justicia[94]. Aún en 2017 las prácticas siguen avanzando y modificándose, pero no existe reporte en el Perú que explique o ejemplifique estas prácticas en nuestro territorio, como si estas no sucedieran o fueran solo problemas que parten de Medio Oriente y no nos afecta. Ya lo dijo la ONU en su informe **«El uso de Internet con fines terroristas»** (2012), que son las redes sociales como Facebook, Twitter y YouTube las utilizadas para llegar a sus potenciales nuevos reclutas, pues estas plataformas representan bajo coste y riesgo, y se encuentran a fácil acceso de la población.

Pero el campo de las redes no es el único utilizado para la captación. Los ciberterroristas utilizan otros medios de comunicación para seguir en contacto y captación. Un estudio publicado por la consultora de seguridad *Flashpoint* (2016) da una lista de las herramientas utilizadas por ISIS para su ejercicio en el ciberespacio; entre ellas, un servicio de aplicaciones de propaganda móvil, lo que permite su expansión de ideología, entre las que se encuentran *The A'maq Agency*, *Al-Bayan Radio*, *Alphabet* y *Voice of Jihad*.

Actualmente, el Perú no cuenta con un estudio que de cifras de cuantas personas han sido captadas por movimiento terroristas o ciberterroristas a través de medios digitales desde el inicio de siglo. No obstante, no podemos descartar que ello es una realidad y que las cifras pueden sorprendernos si efectuamos dicho estudio en los años próximo. El problema que existe en el país es la falta de visión y entendimiento de la realidad nacional y global, al punto que, puedo asegurar, cuando empecemos a tomar cartas sobre el asunto, estos criminales ya estarán familiarizados; y si nace un grupo enteramente ciberterrorista, su comprensión será mayor.

1.3.5. *Gamificación delictiva: Videojuegos en el plan de expansión del ciberterrorismo*

La gamificación es una actividad que permite el aprendizaje rápido de cualquier actividad educativa-profesional. Llevada al ámbito delictivo sus resultados son igualmente proporcionales, y ahora que es empleado por los terroristas, la capacidad de expandir sus ideas y reclutar futuros soldados va en aumento. Sin embargo, el producto de la industria del entretenimiento más rentable del mundo siempre ha estado en debate desde su creación en la década de los 50s —algunos aseguran que sus primeras ideas nacieron en 1912, pero no es una afirmación aceptada por todos, y menos un tema debatible para esta investigación— hasta los días actuales, en los que muchos países siguen debatiendo sobre su contenido violento y

[94] HUERTAS GRANADA, Yenalia (2016). **«La captación de terroristas a través de internet es un riesgo latente»**. 2017, de Granada Hoy. Sitio web: http://www.granadahoy.com/granada/captacion-terroristas-traves-internet-latente-0-1001300178.html

para adultos; pero los videojuegos tienen muchas categorías como en el cine y múltiples calificaciones para cada tipo de cliente, aunque ese no es el tema de fondo. El tema principal es el uso de este medio para experimentos por parte de estos criminales.

Los grupos terroristas —que poco a poco se van trasladando y empleando metodologías ciberterroristas— conocen la fuerza de esta industria y han visto en los videojuegos un buen sistema para la captación de sus actividades. La primera vez que se habló del empleo de elemento del mundo *gamer* fue en un reportaje realizado por la cadena de noticias CNN, donde se informaba que ISIS usaba medios sociales como Instagram para publicar contenido con referencia al juego *Call of Duty*, acompañado de la frase **«Esto es nuestro llamado al deber (Call of Duty) y reaparecemos en Jannah»** (SEGALL, 2014). Ese mismo año apareció un vídeo de una versión modificada del videojuego *The Grand Auto 2004: San Andreas* llamada **«*Grand Theft Auto: Salil al-Sawarem*»** cuyos personajes iban vestidos como soldados del Estado Islámico y donde sus logotipos invadían todos los escenarios, un juego diseñado, según medios de ISIS, para elevar la moral de los *mujaidines* y entrenar a niños y jóvenes para luchar contra Occidente e infundir terror en los corazones de quienes se oponen al Estado Islámico (CROMPTON, 2014). Lo irónico, el empleo de un videojuego occidental para destruir occidente.

Un año más tarde —y días antes del atentado de París— el Ministro del Interior de Bélgica, Jan Jambon, daría información del uso de la consola PS4 de Sony por parte del DAESH como medio de comunicación, debido a su seguridad y el lenguaje encriptado en la jugabilidad *online* (VALERA, 2015), lo que motivo el pronunciamiento de Sony, empresa que admitió que la PS4 podría ser abusada, pero destacó que las características de comunicación de la consola eran comunes con todos los dispositivos modernos conectados (YIN-POOLE, 2015).

> «*PlayStation 4 permite la comunicación entre amigos y compañeros jugadores y, en común con todos los dispositivos modernos conectados, esto tiene el potencial de ser abusado. Sin embargo, tomamos nuestras responsabilidades para proteger a nuestros usuarios con extrema seriedad y exhortamos a nuestros usuarios y socios a informar actividades que pueden ser ofensivas, sospechosas o ilegales. Cuando identificamos o recibimos una notificación de dicha conducta, nos comprometemos a tomar las medidas apropiadas junto con las autoridades apropiadas y continuaremos haciéndolo*»[95].

No pasó mucho tiempo para que un nuevo producto de ISIS se distribuyera en el mundo *gamer*. Empleando un *mod* sobre el juego **«ARMA 3»**, remodelaron las *skins* de los personajes dándoles apariencia de los combatientes del DAESH, situaron la acción en una zona indeterminada

[95] YIN-POOLE, Wesley (2015). **«Sony responds to claim PS4 used for terrorist communications»**. 2017, del portal Eurogamer. Sitio web: http://www.eurogamer.net/articles/2015-11-16-sony-responds-to-claim-ps4-used-for-terrorist-communications

del Oriente Medio, y establecieron nuevos objetivos militares: el ejército sirio, los occidentales y los kurdos se convirtieron en los enemigos a batir; un *mod* que alcanzó popularidad en Internet y que tenía como fin la captación de jóvenes influenciables y accesibles (VILLAMIL, 2017).

He aquí una observación, y es que antes de pensar en que todos los videojuegos por naturaleza son violentos o pueden generar violencia extrema o masiva en sus usuarios, deberíamos conocer más de cerca su mercado, el sistema de clasificación, las desarrolladores y todos aquellos que componen esta industria, que si bien es algo que no es influyente en la investigación, marca el principal objeto de incomprensión sobre los videojuegos, y por qué la presencia del terrorismo en este campo está causando más controversia de las ya existentes. Ya lo dijera Félix Etxeberria, catedrático de Pedagogía en la Universidad del País Vasco, que **«los videojuegos no son causantes de comportamientos agresivos; de lo contrario, todos los adolescentes y jóvenes estarían matando a gente»**[96]. De igual forma Roberto de Miguel, profesor de Teoría de la comunicación de la Universidad Rey Juan Carlos, discute la hipótesis del modelado social, recordando que el primer *Call of Duty* apareció en 2003, y bajo esa hipótesis, hoy tendríamos asesinos en masa y un despliegue de gran violencia social; pero, **«no se aprecia un aumento significativo de la violencia, durante los últimos diez años, en las sociedades donde más se juega a este tipo de juegos»**[97]. Finalmente, Victoria Tur, profesora de la Universidad de Alicante, coincide con los demás investigadores y señala que **«la investigación de los videojuegos violentos no ofrece resultados concluyentes sobre una relación causa efecto»**[98].

Videojuegos de contenido violento siempre han existido. Desde *Death Race* (1976), pasando por *Splatterhouse* (1988), *Mortal Kombat* (1992), *Postal* (2003) hasta las sagas más actuales de *Call of Duty* y *Battlefield*, pero estos no te transformar en un ciberterrorista o te llevan al mundo del ciberterrorismo, y mucho menos te reclutaban a sectas cuya única función era generar violencia. Se pensaría que, con estos antecedentes, ISIS decidió ser pionero y dar paso al campo de la captación por videojuegos; pero el uso de videojuegos como herramienta de reclutamiento no es nuevo. A decir verdad, el Ejército de los Estados Unidos, durante la última década, ha ofrecido el *shooter* multijugador *online America's Army* (2002, 2009, 2013); uno de los juegos de guerra más descargados de todos los tiempos y utilizado para impulsar el reclutamiento de su armada; llegando a instalar estaciones de juego en un centro comercial de Filadelfia en el año 2009, para que los niños puedan jugarlo y, si así lo decidían, hablar con alguien sobre lo que harían con sus vidas en las fuerzas armadas (CASPIAN KANG, 2014).

[96] CANO, Luis (2014). **«De la guerra en los videojuegos a la yihad»**. 2017, del portal ABC internacional. Sitio web: http://www.abc.es/internacional/20141127/abci-violencia-videojuegos-terrorismo-guerra-201411262047.html

[97] **Ibid.**

[98] **Ibid.**

Pero, a pesar de lo dicho al inicio de este punto, la presencia terrorista en los videojuegos se popularizó en 2014. Su verdadera aparición se remonta al año 2006, donde el grupo Al-Qaeda realizó cambios en el FPS *Quest for Saddam* (2003) e introdujo otro juego llamado **«*Quest for Bush*»**. El objetivo del juego original era matar soldados iraquíes y capturar a Saddam Hussein, mientras que Al-Qaeda revirtió por completo los papeles de los jugadores. Además, el artista iraquí estadounidense, Wafaa Bilal, hizo más adaptaciones al mismo juego, que llamó **«*Night of Bush Capturing: A Virtual Jihadi*»** (2008) (CHARLES, 2009).

Sobre el juego **«*Grand Theft Auto: Salil al-Sawarem*»**, no está claro si fue realmente producido o no; ni quién exactamente lo desarrolló, ya que hay muchos enlaces al videojuego, especialmente aquellos que conducen a sitios web de *torrents*. Sin embargo, los enlaces actuales no funcionan o conducen a sitios web maliciosos. Al parecer, el objetivo general de crear y lanzar el videojuego era ganar publicidad y atraer la atención del grupo. Esto es parte de los esfuerzos del grupo Jihad 3.0, ya que el objetivo principal son los jóvenes que podrían tener la impresión de que ISIS es un grupo tecnológicamente avanzado que no solo produce videos de alta definición y bien editados, sino que también posee sus propias aplicaciones, redes sociales herramientas, drones y videojuegos. YouTube sigue siendo una de las principales plataformas en donde ISIS aún comparte y difunde sus mensajes (AL-RAWI, 2016). Por otro lado, esto no elimina lo dicho en esta sección. La presencia de la estructura *gamer* en el ciberterrorismo está presente y cada día se hace más atractiva para captar a más jóvenes a su movimiento. Lo que debemos evitar es que la distribución de este contenido malicioso —en su mayoría, *mods* de juegos actuales o reversiones de *abandonwares*— se siga propagando por la red, y eliminar de una vez por todas la discusión y culpabilidad sobre videojuegos distribuidos por compañías legalmente formadas. El terrorismo ya tiene presencia en la industria más rentable, y pueden seguirles otros sectores, por más que algunos especialistas afirmen que esta no es su necesidad o su campo de acción. Las pruebas hablar por sí solas.

Fotografía en Instagram que hace referencia a un mensaje de ISIS
Fuente: CNN

Captura del *mod* yihadista del videojuego **«ARMA 3»**, que simula la actuación de los grupos armados de DAESH en Irak y Siria
Fuente: www.elimparcial.es

Portada del videojuego **«*Grand Theft Auto: Salil al-Sawarem*»**
Fuente: *Terrorism and Political Violence Journal*

1.4. Antecedentes que reflejan la existencia de la figura del ciberterrorismo a nivel internacional

Uno de los principales sustentos en la lucha contra el ciberterrorismo es la historia de sus ataques que se han producido a nivel mundial. Muchos de ellos aún no son de conocimiento público, ya que son tratados como casos de seguridad nacional por los países afectados, así como por organismos internacionales. Un estudio sobre los principales ataques ciberterroristas producidos a nivel global en los últimos años se presentó durante la conferencia **«De Sendero a ISIS: El peligro del ciberterrorismo y la necesidad de regularizarlo»** (SANTIVÁÑEZ, 2016), exhibida en el Instituto Nacional de Ciencias Penales de México y el *OAS-First Cyber Security Symposium* de la OEA en Colombia, con el fin de dejar en claro que el ciberterrorismo es una amenaza latente y necesita de acción jurídica por muchos países. Es el resultado de este mismo estudio —con información adicional del último año— el que se muestra a continuación.

1.4.1. *En América*

ATAQUES CIBERTERRORISTAS		
PAÍS	**FECHA**	**INFORMACIÓN**
Estados Unidos	2001	Ciberatacantes chinos lanzan un ataque DDoS contra sitios web estadounidenses luego de que se produjera la colisión entre un avión espía naval estadounidense y un avión de combate chino.
	2004	WikiLeaks publica un documento donde se afirma la intrusión por parte de un estudiante en Medio Oriente a los sistemas de la NSA, con el fin de activar el Plan *Star Wars*, una estrategia antibélica instaurada en el gobierno del presidente Ronald Reagan (1983). El atacante redireccionó armas nucleares de EE. UU. a suelo estadounidense, con el supuesto propósito de desaparecer el país. El ataque fue detenido a tiempo y ninguna bomba fue lanzada.
	2008	A partir de un pendrive conectado a una portátil del ejército estadounidense en una base militar de Medio Oriente, se instaló un *spyware* que permitió ejecutar un ataque a los sistemas militares de EE. UU. y transferir información a servidores bajo control extranjero. El *spyware* no pudo ser detectado.
	2009	Por medio de un BOTNET se ejecuta un ataque DDoS a las principales webs gubernamentales, financieras y de noticias de EE. UU. y Corea del Sur. El número de computadoras secuestradas

		varía según cada fuente especializada. El *Security Technology Response Group* de Symantec calculó un total de 50K; el Servicio de Inteligencia Nacional de Corea del Sur, 20K; e investigadores vietnamitas de ciberseguridad, 166K.
Colombia	2012	Se ejecuta un ataque ciberterrorista al gobierno del presidente Juan Manuel Santos y al ejército del mismo país a razón del impulso de una Ley que buscaba penalizar el ciberterrorismo.
Canadá	2011	Ciberatacantes, con direcciones IP de China, se infiltraron en tres departamentos de gobierno canadiense y se auto transmitieron información clasificada. El gobierno interrumpió el acceso a Internet de los tres departamentos para detener la auto transmisión de los atacantes.
Venezuela	2015	Gobierno venezolano demanda a *Dolar Today* (EE. UU.) por publicar diariamente una tasa ilegal de cambio entre el bolívar venezolano y el dólar estadounidense, la que está basada en cálculos especulativos que cifra el dólar 130 veces superior a la tasa de cambio oficial publicada por las autoridades venezolanas, siendo esto (según el gobierno) información falsa que es considerada (por el gobierno) como ciberterrorismo.

1.4.2. *En Europa*

ATAQUES CIBERTERRORISTAS		
PAÍS	**FECHA**	**INFORMACIÓN**
Serbia-Yugoslavia (Guerra de Kosovo)	1999	Se atacaron las computadoras de la OTAN con bombas e-mail y DDoS por su actuación en la Guerra de Kosovo. También se vieron afectados los sistemas de empresas, organizaciones públicas e institutos académicos con correos cargados de virus. Según informes, se cree que algún grupo *hacktivista* fue el responsable.
Estonia	2007	El gobierno de Estonia fue sometido a ciberterrorismo por el NASHI, un grupo pro-Kremlin de Transnistria, quienes emplearon técnicas como inundaciones de ping y BOTNETS para penetrar y derribar sitios web clave del gobierno, dejándolos

		inútiles. Se pensó que el grupo recibió apoyo del gobierno ruso, no solo por sus complicados métodos de ataque; además, porque estos ataques fueron consecuencia de la reubicación en Estonia del soldado de bronce de Tallin y otras tumbas soviéticas.
Rusia-Georgia (Guerra de Osetia del Sur)	2008	Durante el conflicto entre Rusia y Georgia se originaron los primeros estragos de la ciberguerra, en donde ataques masivos a los servidores y webs del gobierno georgiano se produjeron a gran escala, debilitándolo y afectando su capacidad de comunicación con sus ciudadanos y el resto del mundo. No existieron daños ni perdidas físicas.
España	2012	Ciberterroristas *antifascistas* publican datos de clientes de comercios sevillanos para ser objetivos de sus acciones. La coordinadora sevillana contra el terrorismo (CSCT) tuvo conocimiento que varios establecimientos comerciales de moda y *souvenirs* sevillanos, habrían sido víctimas de un ataque a sus webs y bases de datos de clientes con el fin de robar la información de estos, muchos de ellos miembros de las fuerzas y cuerpos de seguridad del Estado —según ha podido saber la CSCT de fuentes de la investigación—, para posteriormente colgarlos en webs y sitios de internet violentos y extremistas vinculados a grupúsculos autodenominados antifascistas, llamando a actuar contra esos clientes de dichas tiendas por comprar prendas o motivos con la bandera de España u otros símbolos históricos españoles.
Gran Bretaña	2013	A través de *Spamhaus*, un servicio de filtrado utilizado para eliminar mails no deseados, se ejecutó un ciberataque en enrutadores de banda ancha para convertir a sus propietarios en participantes inadvertidos. Ese mismo año, *Spamhaus* agregó *Cyberbunker*, un proveedor de servicios de Internet, a sus sitios de la lista negra y esta, junto con otras compañías de *hosting*, contrataron a *hackers* para poner BOTNETS que explotaron en casas de usuarios y enrutadores de banda ancha.

		para cerrar el sistema de *Spamhaus*, como represalia a sus acciones. Este es considerado uno de los ciberataques más grandes de la historia.
Ucrania	2015	El 23 de diciembre, en la región de Ivano-Frankivsk, se produjo un corte de energía eléctrica, producto de un ciberataque masivo que afectó a múltiples compañías del país. Se supo que los atacantes utilizaron el troyano *BlackEnergy* para incorporar el componente *KillDisk* en los ordenadores afectados, impidiendo el reinicio de los sistemas y la portabilidad de códigos específicos para sabotear sistemas industriales. El CERT-UA recibió las primeras denuncias en noviembre del mismo año, informándose que a raíz de esos ataques múltiples documentos gubernamentales y material en vídeo también había sido destruido.

1.4.3. *En Asia*

ATAQUES CIBERTERRORISTAS		
PAÍS	**FECHA**	**INFORMACIÓN**
Sri Lanka	1998	Con el empleo de 800 mails diarios, y por el periodo de dos semanas, las guerrillas étnicas tamiles inundaron la mensajería de las embajadas de Sri Lanka, con el fin de interrumpir sus comunicaciones. Los autores, en su contenido, se denominaron los *Black Tigers* de Internet. Las autoridades de inteligencia lo catalogaron como el primer ataque ciberterrorista del país.
Corea del Sur	2009	Según la Agencia de Ciberseguridad Coreana, 11 sitios web, entre los que figuran el sitio presidencial de la Casa Azul, el ministerio de Defensa, la Asamblea Nacional, el Banco Shinhan y el periódico Chosun Ilbo fueron afectados por un ataque *zombie*, impidiendo su acceso a los mismos.
	2009	Por medio de un BOTNET se ejecuta un ataque DDoS a las principales webs gubernamentales, financieras y de noticias de EE. UU. y Corea del Sur. El número de computadoras secuestradas varía según cada fuente especializada. El *Security Technology Response Group* de

		Symantec calculó un total de 50K; el Servicio de Inteligencia Nacional de Corea del Sur, 20K; e investigadores vietnamitas de ciberseguridad, 166K.
Irán	2010	La instalación nuclear en Natanz fue atacada por un *IWorm* denominado **«Stuxnet»,** una especie de bomba digital que se expandió e infectó más de 60K computadoras de sectores industriales, destruyó 1K centrífugas nucleares de Teberán y retrasó el programa nuclear del país, haciendo sus sistemas inservibles. Se cree que **«Stuxnet»** fue creado por Israel y EE. UU., pero nadie se atribuyó la responsabilidad. Nombres como España, e incluso, el mismo gobierno iraní, aparecieron en la lista de los posibles responsables.
India	2012	A pesar de tener una reputación en el desarrollo de software e informática, *crackers* penetraron cuentas de e-mails pertenecientes a 12K personas. En la lista se encontraban correos de funcionarios del Ministerio del Interior, del Ministerio de Asuntos Exteriores; la Policía Fronteriza Indo-Tibetana (ITBP) y la Organización de Investigación y Desarrollo de la Defensa (DRDO).
Israel	2012	En la víspera del **«Día del Recuerdo del Holocausto»**, individuos y grupos antiisraelíes (**#opiIsrael**) dirigieron un asalto DDoS contra sectores financieros y empresariales, instituciones educativas, periódicos, ONGs y empresas privadas israelíes, con el fin de borrar a Israel de Internet.

1.4.4. *En África*

ATAQUES CIBERTERRORISTAS		
PAÍS	**FECHA**	**INFORMACIÓN**
Mauritania	2010-2015	El grupo terrorista Boko Haram utilizaba Internet para reclutamiento y propaganda; así como desafiar al presidente nigeriano de ese entonces, Goodluck Jonathan, publicando sus reclamos en vídeos.
Sudáfrica	2015	Un informe de *Sunday Times* (UK) señaló que se lanzaron 6K ciberataques contra proveedores de servicios de Internet de

		infraestructura sudafricana (PSI) y diversas empresas del país.

1.4.5. *En Australia-Oceanía*

ATAQUES CIBERTERRORISTAS		
PAÍS	**FECHA**	**INFORMACIÓN**
Australia	2000	El FBI informa que una persona obtuvo el control de una planta de tratamiento de desagüe cloacal y liberó 1M de litros de desechos en los ríos. Se consideró como el primer ataque ciberterrorista en el país.
	2010	La compañía de telecom OCPUS sufre un ataque por parte de China. El país asiático emitió un comunicado aduciendo que fue un ataque por error.
	2011	Ataque al Banco Central de Australia, con el fin de robar información sobre planes económicos de este y otros países. Se culpó a China de los hechos, puesto que el malware utilizado era de origen chino y el mismo también fue utilizado para obtener información sobre las negociaciones del G20 (2011). Este ataque se pudo realizar gracias al envío de e-mails con contenido y asunto que parecía ser legítimo (Asunto: Planificaciones Estratégicas FY2012; emisario: ejecutivo importante del banco de quien no se ha tenido información a la fecha).

1.5. Antecedentes y actualidad de la figura del ciberterrorismo en el Perú. Realidad de su existencia y que pone en alerta a nuestra nación

La presencia del ciberterrorismo en nuestro país se ha pronunciado de diferentes formas, tal cual hemos detallado en el transcurso de esta investigación. No obstante, no existen antecedentes de ataques realizados hasta la fecha. Podríamos suponer que los ataques efectuados al Ministerio del Interior del Perú en el año 2011 es un ataque ciberterrorista, pero no tuvo más fin que el de demostrar la baja defensa cibernética que maneja el Estado.

A la fecha, el ciberterrorismo en el Perú solo se ha manifestado a través de páginas web y redes sociales anteriormente mencionadas. Eso no significa que puede descartarse una amenaza mayor con el paso de los años o de los días, dependiendo que tan creciente se mantenga la debilidad jurídica, política, social y de seguridad en el país..

1.6. La responsabilidad del Perú ante la amenaza ciberterrorista

Si bien no existe registro de ataques con fines terrorista en el Perú, su presencia ya habita en la estructura de Internet desde ya tiempo. Estamos ante una nueva forma de lucha contra la estructura terrorista y subversiva, que no se siente debilitada por los avances tecnológicos, sino los aceptan como una ventaja a bajo costo para sus fines ideológicos. Es así como podemos englobar tres tipos de responsabilidades para que el Perú, una vez más, le haga frente al terrorismo que ahora se maneja por el mundo de Internet, el ciberterrorismo que cala adeptos con el paso de las horas y que se ha vuelto un ambiente ignorado por políticos, abogados y cierto sector de las fuerzas del orden.

1.6.1. *Responsabilidad social*

La lucha que se entabló contra el terrorismo desde la década de los 80s en el Perú nos lleva a un compromiso u obligación para con la sociedad. Es esta misma responsabilidad la que nos permite generar una mejor sociedad modelo y segura para vivir. De nosotros depende generar esa sociedad en donde la convivencia y el respeto a las normas y los DD. HH. sea un factor predominante.

Ante un componente que no permita la convivencia, que esté en contra de nuestros valores morales y sociales, aunque la respuesta pueda ser dura o genere múltiples debates, no debe caber la duda en su retiro de la sociedad antes que la corrompa por completo. De igual forma, todas aquellas conductas de las que seamos testigos en la red y que pretenden dar paso al ciberterrorismo, debe ser denunciadas a las autoridades competentes.

Parte de nuestra responsabilidad social es recuperar la educación de los jóvenes y darles el conocimiento sobre los hechos que lastimaron a la república, para que el duro golpe que sufrieron las generaciones el siglo pasado no marquen a las actuales y a las que vendrán. Como dijera el filósofo Jorge Agustín Nicolás Ruiz de Santayana: **«Aquel que no conoce su historia está condenado a repetirla»**.

Con estos principios, es posible incluso combatir la **INSEGURIDAD CIUDADANA** que se vive en el país. La unión de fuerzas políticas, sociales y estatales puede llegar a formar un primer camino en esta lucha, y también, cimentar el camino para contrarrestar los avanzases del ciberterrorismo. El factor social es importante.

1.6.2. *Responsabilidad moral*

Cada uno de los peruanos es responsable de cada una de las acciones que se produzcan en el futuro de la nación. Se ha trabajado en economía, turismo y gastronomía, creando un efecto de unión social que parece más latente con los deseos de otros de ser dueños del pisco o cuando de futbol se habla; pero hemos quedado estancados en la cuestión política con altos

índices de corrupción y gobiernos que la han abandera hasta hoy en día. El crimen organizado se sigue produciendo en masa e invade más terrenos, desde aquellas zonas de la ciudad que se consideraban muy seguras, hasta la red de redes. La falta de oportunidades, los débiles programas de rehabilitación y resocialización penitenciaria, el nulo apoyo a las víctimas, la baja educación y los pocos intereses del Estado por ver al país en su total desarrollo y no en una inacabable centralización aumentan la perspectiva delictiva n el país y se transforman en nuevos caldos de cultivo para el crimen.

Como ciudadanos, no se debe permitir que estas acciones se mantengan por mucho más tiempo. Por situaciones similares se abrió puerta para que aparezcan los movimientos subversivos y el terrorismo. Hoy, está cada vez más cerca un rebrote con la fórmula y presencia del ciberterrorismo.

Se debe exigir a las autoridades que se cumplan las normas, empezando por ellos, y luego, con esa misma fuerza, que se cumplan las normas contra el crimen organizado y se sienten bases para la lucha contra la figura del ciberterrorismo. No podemos permitir que el pase de esta figura siga su crecimiento acelerado y, como ciudadanos, no respondamos ante nuestra responsabilidad de cuidar a nuestra nación, porque la seguridad y el cumplimiento de las normas es dependencia de todos, y no solo de las esferas de poder. La moral que aún no quede ayuda a combatir un mal que no debe proliferar.

1.6.3. *Responsabilidad histórica*

Quizás la más importante de todas y la que contiene nuestras experiencias, éxitos y fracasos. Los hechos históricos nos levantaron como los victoriosos ante el terror y su ideología destructiva, pero no eliminaron de sus páginas a las muertes de soldados e inocentes, ni de su reflejo en la historia de la humanidad. Por algún factor desconocido, somos nosotros quienes hemos pretendido olvidar lo pasado y generar un futuro con páginas vacía y que eran importantes.

La sombra del terrorismo aún está vigente en el país, y no porque lo diga el informe elaborado por la Comisión de la Verdad y Reconciliación, sino por las muestras de vandalismo, pinturas en la Universidades, el contenido web, la presencia en las redes sociales y el desconocimiento de los jóvenes de los hechos criminales, culpa nuestra por extirpar la lucha contra el terrorismo de nuestra propia historia nacional.

Se ha olvidado que por más de veinte años se escribieron los capítulos más duros y sanguinarios de nuestra historia; que hasta fin de siglo fueron dos los grupos que controlaban el libre tránsito de la ciudadanía y fundaban el terror; que más de 25mil peruanos perdieron la vida; y que las pérdidas económicas ascienden a más de US$25M (veinticinco y 00/100 millones de dólares americanos); que aparecieron los jueces sin rostro porque era difícil juzgar a un terrorista que los amenazaba a ellos y a su familia, si

solo tentaba con encerrarlo en prisión; se olvidaron del atentado en Tarata (1992) y la toma de la Embajada de Japón (1996); se olvidaron del asesinado por el grupo terrorista de turno de un policía que estaba controlando el tránsito en una de las tantas calles de Lima, un policía que solo fue parte del *aniquilamiento selectivo* de un *perro sarnoso de la reacción, guardián del viejo y caduco Estado*[99].

Nuestro deseo de borrar ese pasado que es parte de nuestra historia, nos ha llevado a que actualmente se genere un desconocimiento por parte de los jóvenes que alguna vez se pensó proteger, y que ahora exigen la liberación de uno de los principales cabecillas terroristas como lo es Abimael Guzmán. La historia puede cambiarse. El Perú logró una vez vencer al terrorista y puede volver a hacerlo, pero debe aceptar su historia como tal, y la responsabilidad que esta trae consigo.

2. Planteamiento teórico

2.1. Análisis: La normativa peruana e internacional en referencia a la figura del ciberterrorismo

No existe una norma en el Perú que considere al ciberterrorismo como una amenaza, muchos menos como un delito. No existe proyecto de Ley que siquiera plantee esta posibilidad, y las modificatorias presentadas al código penal peruano hasta mitades del año 2017 no la han incluido más que en su vertiente de apología, llamándola todavía apología del terrorismo. Esto no es suficiente.

Aún no ha habido un acto de ciberterrorismo con daños físicos y efectos materiales, pero la tecnología de los ciberataques está evolucionando claramente desde una simple molestia a una amenaza seria contra la seguridad de la información e incluso contra infraestructuras nacionales esenciales[100], acciones que ya se materializaron en algunos países tan poco desarrollados o más desarrollados que el nuestro.

Nuestras contrapartes internacionales vienen avanzando en esta problemática desde hace muchos años, y hoy se pueden observar frutos de progreso en materia de ciberseguridad; no obstante, el mayor obstáculo que ofrece este tiempo al universo jurídico es la falta de armonización sobre el cibercrimen. Si bien es cierto que la apología del terrorismo por medios digitales ya está tipificada en la mayoría de las plazas europeas como un delito penal susceptible de ser perseguido (CALDERÍN & JIMÉNEZ, 2016), la lucha completa contra lo ciberdelitos solo se constituye de acuerdos bilaterales y unilaterales que hablan de elementos penales y procesales penales, pero que no contempla a muchos países asiáticos y latinos. Y con relación al ciberterrorismo, existe una tendencia

[99] JIMÉNEZ BACA, Benedicto (2000). *Capítulo I: Denominación, antecedentes Históricos, Objetivos, Basamento Ideológico Político, Planes y Campañas*. **«Inicio, Desarrollo y Ocaso del Terrorismo en el Perú. El ABC de Sendero Luminoso y el MRTA ampliado y comentado – Tomo I»**. Pp. 85. Lima, Perú. Editorial Sanki.

[100] THEILER, Olaf (2000). **«Nuevas amenazas: el ciberespacio»**. 2017, de Revista de la OTAN edición digital. Sitio web: https://www.nato.int/docu/review/2011/11-september/Cyber-Threads/ES/index.htm

a la adaptación de normas establecidas en leyes contra los ciberdelitos para considerarlos actos ciberterroristas. Es el caso de España, país que adapta su código penal y sus artículos relacionados a los ciberdelitos[101] con inclinaciones al ciberterrorismo; o la Ley de ciberdelitos de Venezuela (2001), que establece que, dependiendo de su origen, motivación y fin, varios delitos pueden catalogarse como ciberterrorismo Diferente es la visión de EE. UU., país que durante el mandato del presidente Barack Obama propusieron la creación de una organización similar a la NCTC y que estuviera orientada, de manera exclusiva, a la lucha contra el ciberterrorismo y los ciberataques, los que han demostrado tendencia creciente en los últimos años (NAKASHIMA, 2015)

Pero lo cierto es que el trabajo colaborativo y lo parámetros que brindan las Guías de la OCDE para la seguridad de los sistemas de información y redes (2003); el Convenio de Budapest (2004); el Convenio del Consejo de Europa para la prevención del terrorismo (2005); el Manual de Tallín de legislación internacional aplicable a la ciberamenazas de la OTAN (2012); la Estrategia de Seguridad Cibernética de la Unión Europea para un ciberespacio abierto, seguro y protegido (2013); así como los informes de la ONU, 55/63 (2001), 56/121 (2002), 57/239 (2003) y 58/199 (2004); buscan propiciar un avance jurídico en la materia de seguridad y lucha contra el cibercrimen, entre los que podríamos considerar el ciberterrorismo. Aunque algunos de estos trabajos no lo mencionen esta figura, y a pesar que el principal problema que radica en muchos países es la falta de iniciativa por buscar una legislación que permita la lucha contra el ciberterrorismo, algunos académicos y especialistas en el tema consideran que esto no es necesario, ya que los acuerdo y adaptaciones sistemáticas no escritas como norma para hacer frente a este nuevo tipo de terrorismo son suficientes, especialmente porque lo ciberterroristas operan de forma anónima y en un mundo sin fronteras en el que el estado de derecho no se aplica (WAGNER, 2017); afirmación con la que se discrepa en este trabajo.

Si aceptamos como desventaja el anonimato y la vulnerabilidad que existe en Internet, esto asociado a la débil y escasa experiencia en ciberdefensa de muchos países —entre ellos, el Perú—, no podremos dar un verdadero avance progresivo. Cuando se ha buscado la normatividad de conductas generadas con el uso de las tecnologías se ha confundido con el mal llamado gobierno de Internet, olvidando que se rige por una gobernanza y es la nueva tendencia que marca el desarrollo progresivo de las naciones. Si pensamos que no podemos regular las conductas delictivas que se producen en el ciberespacio, vamos en contra de las corrientes antes mencionadas y que generaron convenios de colaboración múltiple. Si pensamos aún con el Derecho tradicional, en donde la territorialidad es determinante para combatir la delincuencia —elemento razonable—, no podremos ver más allá de los límites de la bandera, límites que han demostrado que no es necesaria la presencia física de un delincuente para causar estragos en los sistemas de un país o en la población misma.

La legislación del ciberterrorismo constituye hoy uno de los últimos retos —y quizás, el más importante— que el Derecho tendrá que afrontar. Entre más rápido pasa el tiempo y entre más compleja se hace la tecnología, más complicado se

[101] Cfr. Artículos 573; 573.2; 578 y 579 del Código Penal Español.

hace el trabajo legislativo. Sobrepasar los límites es una clave que puede ayudar al Perú en los años venideros. Recordemos que, si bien los ciberterroristas mantienen comunicación y actividades en el mundo de la web, otro gran porcentaje de sus actividades navega en la Deep web y Dark web, a las que se tiene acceso gracias a la red TOR y el (punto)onion; entre otros canales igual de ingeniosos.

Este es el nuevo reto del Derecho, reto que fue impuesto hace más de 10 años y que aún no tiene una respuesta jurídica clara. La lucha contra el cibercrimen puede llegar a ser tediosa y compleja, pero la respuesta legal no debe quedar en meras intenciones o en intentos fallidos. Una nueva oportunidad para el Perú llega en el lenguaje de la tecnología. Quizás, solo quizás, un trabajo que permita establecer las bases para buscar la legislación que permita tipificar la figura del ciberterrorismo puede ser el primer paso para la tan ansiada presencia en el Convenio de Budapest.

2.2. Análisis y explicación de las principales organizaciones a nivel internacional en referencia a la peligrosidad de la figura del ciberterrorismo

Los principales organismos internacionales también se han pronunciado con relación al ciberterrorismo, ya sea por medio de entrevistas o congresos, como informes en materia de cibercrimen y otros. Cada uno de ellos guarda una participación especial y un punto de vista particular entendible de acuerdo con las labores que ejecutan, pero también con un punto en común. He aquí las opiniones recolectadas de cada una de estas instituciones.

2.2.1. *Organización de las Naciones Unidas (ONU)*

Con 193 Estados Miembros, esta organización que nació al finalizar la II Guerra Mundial es la mayor organización internacional y es vista como una asociación de gobierno global que coopera con el derecho internacional, el desarrollo económico, los DD. HH., la paz y seguridad internacional. Bajo este concepto, el ciberterrorismo forma parte de uno de sus principales temas a tratar en cada reunión; especialmente, luego de la creación del Comité contra el Terrorismo tras los ataques terroristas perpetrados el 11 de septiembre en EE. UU.

Al aceptar al ciberterrorismo como un peligro con el que convivimos día a día, la ONU solicita constantemente a los gobiernos a estar preparados y a mejorar en sus estrategias de lucha; especialmente porque los activistas y grupos terroristas se han visto beneficiados de la inexistencia de una estructura internacional que luche con eficiencia contra esta amenaza (MICO, 2012). Esta recomendación es resultado de los múltiples trabajos que ha venido desarrollado el organismo; como el informe elaborado por la UNODC el 2006, resultado del **«Foro sobre el delito y la sociedad»**, en donde señalaban que, como el mundo había evolucionado hacia una economía mundial en los últimos 50 años, la metodología terrorista también se había modernizado, desde armas más complejas hasta el

ciberterrorismo, quedando todos los países vulnerables. En el 2009, se habló en el informe del CTITF denominado **«Report of the Working Group on Countering the Use of the Internet for Terrorist Purposes»** de 4 usos de Internet con fines terroristas: (1) Para realizar ataques mediante alteración remota de información o interrupción del flujo de datos; (2) Como fuente de información; (3) Como medio para difundir información relevante de sus finalidades; (4) Como medio para apoyar redes y comunidades dedicadas a perseguir o apoyar actos de terrorismo.

Para el año 2013, la UNODC, con su informe denominado **«El uso de Internet con fines terroristas»**, explica que este es un fenómeno que se propaga con rapidez y exige una respuesta dinámica y coordinada de los Estados Miembros, haciéndose necesaria la capacidad de los sistemas nacionales de justicia penal para aplicar las disposiciones de los instrumentos jurídicos internacionales contra el terrorismo, y así desarrollar mejores conocimientos jurídicas y más especializados, toda vez que este es un peligro que transgrede los territorios nacionales.

En 2015, durante la XXV sesión anual del *Model United Nations International School of The Hague*, cuando se habló de ciberterrorismo, se dejó en claro que uno de sus atractivos es el bajo costo a comparación del terrorismo tradicional, solo dependiendo de una conexión a Internet y la capacitación de reclutas para hacer efectivos sus propósitos; además, se reconoce como la mayor ventaja la inexistencia de regulación, el anonimato, el rápido flujo de información y las grandes audiencias listas para su próximo espectáculo (AKATI-UDI, 2015).

Finalmente, tanto en el 12º y 13° Congreso de las Naciones Unidas sobre Prevención del Delito y Justicia Penal (BRASIL, 2010) (QATAR, 2015), el terrorismo y su evolución continúo siendo un tema de conversación, exhortaron a los países miembros que no habían tomado en cuenta la ratificación de instrumentos contra el terrorismo, así como la implementación de recursos humanos y económicos, los programas de fomento de la capacidad y actividades de capacitación de los funcionarios de la justicia penal, y cualquier medida que resulte pertinente, tengan la voluntad de hacerlo, más aún cuando la ONU cuenta con los medios para apoyar a cada uno de sus países miembros.

En conclusión, la ONU es uno de los organismos internacionales más preocupados por el avance del terrorismo cibernético en los últimos años. Los consideran una rama evolutiva del terrorismo tradicional que exige la creación de nuevas normas y respuestas efectivas de la justicia penal, de capacitación y de trabajo colectivo para hacerle frente al más grande desafío transnacional que se ha tenido en los últimos años. Es por ello por lo que en junio de 2017 se llamó a combatir el ciberterrorismo con 3 actores: La iniciativa privada, los gobiernos y las ONGs, dando un factor de unidad necesario para contraatacar, ya que la independencia y el unilateralismo condenarían al fracaso a cualquier país (SAGNELLI, 2017). En palabras de Ban Ki-moon, ex secretario de la ONU, **«Internet es un excelente ejemplo de cómo los terroristas pueden actuar de**

manera verdaderamente transnacional. En respuesta a ello, los Estados deben pensar y funcionar de manera igualmente transnacional».

2.2.2. *Organización del Tratado del Atlántico Norte (OTAN)*

Desde hace años, la OTAN viene discutiendo sobre el ciberterrorismo en distintos foros relacionados al terrorismo y la ciberseguridad; incluso se ha atrevido a afirmar que esta es una gran amenaza solo comparable con los ataques con misiles, viéndonos en la necesidad de adoptar una estrategia de ciberdefensa mundial (JOHNSON, 2008). Suleyman Anil, quien fuera jefe del Centro de Coordinación de Capacidad de Respuesta a Incidentes de la organización, afirmó en 2008 que un ciberataque determinado en la infraestructura en línea de un país sería **«prácticamente imposible de detener»**, recordando los ciberataques en Estonia en 2007, mismos que derrumbaron los sistemas financieros y estatales, generando consecuencias muy graves (HEATH, 2008). Sin embargo, estas opiniones discrepan de lo dicho por Gábor Iklódy, secretario general adjunto para los desafíos emergentes de seguridad en la OTAN, quien afirmara que **«la capacidad de hacer daño sigue siendo principalmente con los estados nación»**, en lugar de con las facciones ciberterroristas; pero advirtió que era solo una cuestión de meses o años hasta que los terroristas tuvieran los recursos para llevar a cabo ataques cibernéticos contra la infraestructura nacional (BREWSTER, 2012), efecto que se volvió real.

En la actualidad no es desconocido que la OTAN juzga al ciberterrorismo como una amenaza global y contra la que se ha venido preparando desde sus apariciones en los años 80, aconsejando siempre a sus países miembros que tomen las medidas necesarias para hacerle frente. Es a raíz de ello que, en noviembre de 2010, los líderes de los países miembros buscaron impulsar la colaboración para combatirlo (EUROPA PRESS, 2010); en julio de 2016, los Aliados reafirmaron el mandato defensivo de la OTAN y reconocieron el ciberespacio como un dominio de operaciones en el cual la OTAN debe defenderse tan efectivamente como lo hace en el aire, en tierra y en el mar[102]; y en junio de 2017, optaron por convertir el ciberespacio en un dominio operacional oficial de la guerra, junto los otros tres mencionados, como una medida a los ciberataques que siguen en crecimiento, con un aumento aproximado del 60% con relación al 2015 (BROWNE, 2017).

Es innegable que el ciberterrorismo es un peligro para la sociedad, especialmente porque las TIC desempeñan un papel crucial en la búsqueda de la modernización. Esto demanda una clara inversión en el desarrollo de la tecnología cibernética, la que se ha convertido en el área dominante para la interacción política, económica y social, campos que el ciberterrorismo entiende como ventajosos para sus acciones y que la OTAN busca proteger a través de la colaboración múltiple de sus países miembros y la

[102] NORTH ATLANTIC TREATY ORGANIZATION. **«Cyber defence»**. 2017, de NATO. Sitio web: https://www.nato.int/cps/en/natohq/topics_78170.htm

capacitación en temas se seguridad. Entendiendo lo dicho en el 2008, **«el ciberterrorismo solo es comparable con los ataques por misiles»**. En este tiempo, posiblemente, ya lo superaron.

2.2.3. *Comité Interamericano contra el Terrorismo (CICTE)*

Establecida en 1999 mediante la resolución AG/RES. 1650 (XXIX-O/99), está integrado por todos los Estados Miembros de la OEA y organiza una Sesión Regular anual, u foro de discusión y toma de decisiones en temas de contra terrorismo, medidas y cooperación[103]. El Secretario General de la OEA designa al Secretario del CICTE para dirigir la Secretaría, la cual está localizada en las oficinas principales de la OEA en Washington, D.C., con el fin de cumplir con los mandatos establecidos por los Estados Miembros en el Plan de Trabajo del CICTE, la Secretaría[104]:

- Proporciona soporte técnico y administrativo para las sesiones del CICTE y mantiene la comunicación y coordinación entre las sesiones.
- Proporciona asistencia técnica y capacitación a los Estados Miembros en respuesta de sus necesidades y solicitudes.
- Coordina con otras organizaciones internacionales, regionales y subregionales.

Con el paso del tiempo, CICTE ha presentado estudios que han demostrado a los países miembros la existencia del ciberterrorismo y el empleo de las tecnologías por parte de grupos terroristas, que han permitido su mayor crecimiento y amplitud de ideologías. En respuesta, desarrollaron estrategias de capacitación en protección de infraestructura critica, fortalecimiento de estrategias ante amenazas terroristas emergentes, y coordinación y cooperación internacional para sus países miembros, así como campañas de sensibilización en materia de buenas prácticas y prácticas seguras para el uso de las TIC como respuesta ante esta amenaza. Por si fuera poco, desde el año 2008, se desarrolló un proyecto piloto que une a cinco CSIRT a través de un servidor seguro albergado en la OEA para hacer frente a las amenazas terroristas.

Desde 1999, como consta en el documento **«Cooperación hemisférica para prevenir, combatir y eliminar el terrorismo»** - AG/RES. 1650 (XXIX-O/99), se deja en claro que existen tecnologías que pueden ser utilizadas por los terroristas, así como la necesidad de continuar fortaleciendo los mecanismos bilaterales, subregionales, regionales e internacionales de cooperación, señalado en la **«Declaración de San Salvador sobre Seguridad Ciudadana en las Américas»** - AG/DEC. 66 (XLI-O/11). Por otro lado, CICTE reconoce que sus Estados Miembros

[103] COMITÉ INTERAMERICANO CONTRA EL TERRORISMO. **«Estructura y Funciones»**. 2017, de OEA. Sitio web: http://www.oas.org/es/sms/cicte/acerca_nostros_funciones.asp

[104] **Ibid.**

usan cada vez más información e infraestructura TIC, redes, sistemas y tecnologías relacionadas, e integración a Internet global, que esto aumenta el impacto potencial de amenazas de ciberseguridad y explotación de vulnerabilidades (CICTE/DEC.1/12), lo que compone una ventaja para las actividades ciberdelictivas, entre las que se halla el ciberterrorismo.

Como punto conclusivo, CICTE no solo reconoce la existencia del ciberterrorismo, sino que aconseja a sus países miembros a tomar las precauciones para hacer frente a los ciberataques, así como ejecutar respuestas inmediatas que no afecten tanto a su nación. A razón de ello, por medio del **«Programa Integral de Fortalecimiento de la Seguridad Cibernética de las Américas»**, y con el apoyo financiero de los Gobiernos de EE. UU., Canadá, España, Estonia e Inglaterra, así como del sector privado, se ha contribuido a fortalecer las capacidades de los Estados Miembros para detectar amenazas cibernéticas y prevenir, responder y recuperarse de incidentes cibernéticos (CICTE/doc.5/17).

El ciberterrorismo sigue siendo una amenaza latente y en constante crecimiento, que pone en peligro no solo a las infraestructuras críticas, también a la sociedad en general. CICTE reconoce este avance así como su constante amenaza, por lo que ha optado por la capacitación y la colaboración como principal contrataque, objetivos que viene logrando no solo con lo mencionado en el párrafo anterior, también con la Red Virtual Hemisférica de CSIRTs (www.CSIRTAmerica.org) y los aportes para el Manual de Tallin 2.0.

2.2.4. *Agencia Central de Inteligencia (CIA)*

Siendo esta una de las mayores agencias de inteligencia del mundo, la misión de la CIA incluye recopilar y analizar información sobre temas de seguridad nacional de alta prioridad como el terrorismo internacional, la proliferación de armas de destrucción masiva, ciberataques, crimen organizado internacional y tráfico de narcóticos, conflictos regionales, amenazas de contrainteligencia y los efectos de las amenazas ambientales y naturales desastres[105]. Con relación al ciberterrorismo, su visión es más bélica que el de las otras organizaciones, considerando que para hacerle frente tenemos que disponer de tiempo —que es muy corto— y preparación. Toda esta visión se puede apreciar en el *Global Trends* 2030, un reporte de predicciones publicado el 2013 por el NIC y que no solo acepta al ciberterrorismo como un delito global, también señala tomará mayor fuerza con el pasar del tiempo y el avance tecnológico de la humanidad, afectando a las sociedades y sus principales economías, desatando una ciberguerra sin límites.

[105] Cfr. CENTRAL INTELLIGENCE AGENCY. Sitio web: https://www.cia.gov

El informe recomienda a la población global —no solo instituciones armadas— iniciar un proceso de preparación, puesto que reafirma su presencia en el ciberespacio, y que para el 2030 será un delito imparable y con poderío absoluto, pues ya habrán comprendido y dominado los medios digitales, así como descubierto las posibilidades de desbalance económico y social que pueden generar.

«Hasta la fecha, la mayoría de los terroristas se han centrado en causar bajas masivas, pero esto podría cambiar. El futuro incluirá grandes vulnerabilidades: sólo un pequeño número de personas podrían entender los sistemas cibernéticos críticos, por ejemplo, creando un riesgo de que puedan vender sus servicios al mejor postor, incluyendo terroristas que se centran menos en gran número de víctimas y más en extenso perturbaciones económicas y financieras», se señala en uno de los párrafos del capítulo *More weapons and targets in the future* de este informe.

Pero esta no ha sido la única vez que la agencia o alguno de sus miembros —o ex miembros— se han pronunciado con relación al ciberterrorismo. En el Global Trends 2015 (2000), ya se hablaba de un terrorismo trasnacional, de la explotación a la vulnerabilidad de infraestructuras críticas y de la alta interconectividad como ventajas para los ciberataques, dando claros rasgos de lo que es el ciberterrorismo. Quince años después, el ex director Barry Royden, mencionó que el ciberterrorismo era la próxima gran amenaza, especialmente porque vivimos en una sociedad interconectada al extremo (FISHER, 2015). En ese mismo año, el ex director de la CIA, John O. Brennan, dio paso a la creación de una división especial para llevar a cabo el ciberespionaje para hacer frente a los ataques cibernéticos y al ciberterrorismo, una amenaza a largo plazo (BENNETT, 2015); y que, incluso, con el empeño de las tecnologías, grupos como ISIS pueden usarlas coordinar operaciones, atraer nuevos reclutas, difundir propaganda e inspirar a simpatizantes de todo el mundo a actuar en su nombre (HATTEM, 2015).

La lucha contra el ciberterrorismo por parte de la CIA aún no termina. La agencia aprovecha cada oportunidad para aconsejar a las fuerzas políticas y el sector militar de su país a estar preparados ya generar políticas de prevención. A nivel global, recomienda lo mismo para todos los países sin excepción, pues considera que, luego del año 2030, no habrá cura contra esta epidemia.

2.2.5. *El Instituto Nacional de Ciberseguridad de España (INCIBE)*

Aun siendo un organismo dependiente de Red.es (www.red.es) y del Ministerio de Energía, Turismo y Agenda Digital de España, INCIBE es una de las instituciones más preocupadas por la ciberseguridad a nivel mundial y promotora de múltiples eventos y capacitaciones tales como el *Summer bootcamp*; ENISE y el *cybercamp*, que cuentan con el respaldo de organizaciones como la OEA, la INTERPOL, el BID entre otros.

Como parte de esta estrategia de avance tecnológico, en el año 216, publica con el BOE, el primer código español de Derecho de la Ciberseguridad, un documento que recopila legislación española con relación a la ciberseguridad y seguridad de la información, y en cuyo contenido puede encontrarse normativa referente a la regulación de la protección de las infraestructuras críticas, la protección de datos, derecho penal y ciberdelitos, ciberterrorismo, entre otros. Es en este último donde centramos la atención, pues la visión de INCIBE es de objeto social y empresarial, entendiendo que el ciberterrorismo puede atacar ambos flancos y desestabilizar al Estado y sus economías.

Dentro de este escenario de lucha contra el cibercrimen y el ciberterrorismo, INCIBE considera necesaria la capacitación de los agentes jurídicos en los aspectos técnicos y normativos relativos a la ciberseguridad, así como de abogados y todos aquellos que participen de este contexto. Con la creación de dicho código, el trabajo debe ser más simplificado.

Queda claro —y no solo con el documento producido— que la institución española clasifica al ciberterrorismo dentro de las figuras que atentan contra la ciberseguridad de su nación y parte de los nuevos riesgos de la globalización; también aconseja la protección de las infraestructuras críticas, puntos vulnerables de las naciones y principales focos de ataques de los ciberterroristas. Por su lado, INCIBE continuará apoyando la capacitación global de los diversos sectores participantes en la lucha contra el cibercrimen y el ciberterrorismo, como son la policía y el sector jurídico, pues es consciente que esta amenaza es transnacional, y las respuestas deben de manejarse de la misma manera.

2.2.6. *Organización Internacional de Policía Criminal (INTERPOL)*

La organización internacional de policía criminal es el mayor organismo policial del mundo. Creado en 1923 cuenta en sus filas con un total de 192 países, y tiene como misión la comunicación policial para un mundo más seguro, previniendo o combatiendo la delincuencia internacional, la misma que han aceptado se ha expandido a Internet y que ahora tiene mayor poder transnacional. Es dentro de esta nueva estirpe delincuencial en donde han ubicado al ciberterrorismo, pero como parte de la figura ya existente de terrorismo, como una vertiente apoyada en las tecnologías.

Las actividades de INTERPOL se centran en tres programas mundiales de delincuencia: lucha contra el terrorismo, crimen organizado y emergente, y ciberdelincuencia[106]. Cada uno de estos programas cuentan con una estrategia aplicable de cinco años (2016-2020), las que evolucionan a la par de estas figuras delictivas. En cuanto al terrorismo, busca prevenir actividades terroristas actividades a través de la identificación de sus miembros en redes terroristas y sus afiliados, centrándose en cuatro

[106] INTERPOL (2017). **«Global counter-terrorism strategy»**. [Summary]. Pp. 4

regiones que actúan como zonas de coordinación para sus actividades: África, Oriente Medio, Asia y Europa[107].

Es importante resalta que, a pesar de que muchos países miembros no manejan una legislación que entienda al ciberterrorismo como un delito, la INTERPOL lo considera como tal, dentro del rango de ciberdelitos: por lo tanto, parte del área de crímenes de rápido crecimiento gracias al apoyo de Internet y las tecnologías, lo que hace que su naturaleza transfronteriza sea compatible con la naturaleza de la organización, lo que no significa que la labor sea más sencilla. A decir verdad, Jürgen Stock, secretario general de la INTERPOL, ha reconocido anteriormente que la organización anda retrasada en el fortalecimiento de sus actividades cibernéticas (EFE, 2016); esto debe de ser tomado como un llamado a la colaboración de todos los países que la integran.

Finalmente, la organización opina que el uso de las tecnologías en el campo del terrorismo permite los delincuentes facilitar sus actividades y maximizarlas empleando menos tiempo y esfuerzo, siendo amenazas reales para la seguridad de los gobiernos, las empresas y las personas; esto pudo comprobarse en el campo de la delincuencia común tras el ciberataque mundial llevado a cabo mediante el programa de chantaje WannaCry, que ha afectado a numerosos países de Europa[108]. De igual forma, expresan que este nuevo panorama exige una aplicación adecuada de la Ley y conocimientos técnicos, así como otras habilidades necesarias. El arma más eficaz para combatir la delincuencia transnacional y el terrorismo es el intercambio constante de información entre los servicios policiales[109].

2.3. Análisis y explicación de principales empresas de ciberseguridad a nivel internacional en referencia a la peligrosidad de la figura del ciberterrorismo

No solo los organismos internacionales se han pronunciado con relación al ciberterrorismo. Empresas dedicadas al mundo de la ciberseguridad y tecnología también han vertido sus opiniones sobre esta amenaza, ya sea por medio de la elaboración de informes especializados, reportes, congresos, notas periodísticas o *webinars*. Es así como, para esta sección, se ha recolectado la mayor cantidad de información de estas instituciones y se ha resumido en párrafos puntuales.

2.3.1. *ESET (Eslovaquia)*

Esta compañía de ciberseguridad —fundada en 1992— no tiene reportes escritos o compartidos; pero sí cuenta con una producción de artículos publicados en su blog corporativo que dan pistas acerca de su visión sobre

[107] **Ibid.** Pp. 2

[108] INTERPOL (2017). **« Los peligros del terrorismo y la ciberdelincuencia para la seguridad en Europa, temas centrales de una reunión de INTERPOL»**. De Interpol, *Centro de Prensa*. Sitio web: https://www.interpol.int/es/Centro-de-prensa/Noticias/2017/N2017-064

[109] **Ibid.**

el ciberterrorismo y la cibercriminalidad. En 2009, David Harley, actual *senior research fellow* de la empresa —en ese entonces, *Director of malware intelligence*— hablaba de un terrorismo asociado a la desfiguración de sitios web y la denegación de servicio, esperando que en unos años su estructura fuera más personalizada y evolucionara. Esto se pudo ver un año después, cuando la empresa calificó de ciberterrorismo el ataque Stuxnet.

ESET acepta al ciberterrorismo como una amenaza de constante evolución, parte total de la cibercriminalidad y que afecta a los sistemas críticos, tanto estatales como industriales. El empleo de sus actividades no discreparía de las manejadas por el cibercrimen, como es el empleo de malware o el ataque DDoS; pero cabe resaltar —aunque esto no se mencione directamente— que sus motivaciones siempre son diferentes.

2.3.2. *Kaspersky (Rusia)*

La compañía de Yevgueni Kasperski tiene 20 años de experiencia en el mercado de la ciberseguridad y presencia en aproximadamente 200 países del mundo. Para ellos, el ciberterrorismo no es algo ajeno a la seguridad empresarial y gubernamental, considerándolos objetivos naturales de este proceso, al cual han enlazado con la ciberguerra. Aunque su visión sigue siendo más industrializada, no han dejado de aconsejar a los Estados a prepararse, pues consideran que este es el momento para proteger a la ciudadanía y a su infraestructura crítica.

A decir verdad, en una entrevista realizada para el documental Amenaza Cyber del programa La 2 de la cadena TVE de España (2012), Yevgueni Kasperski aseguraba que vivíamos en una ciberguerra constante, dominada por verdaderos especialistas en el campo digital, una ciberguerra que podría causar una Hiroshima digital —haciendo referencia al trágico acontecimiento de la II Guerra Mundial— y dejar el planeta como hace 200 años, abandonado de la tecnología y las interconexiones. Lo más llamativo es que Kasperski no habla de un futuro por llegar, sino de un futuro presente en nuestra sociedad desde hace años.

2.3.3. *Microsoft Digital Crimes Unit (EE. UU.)*

Microsoft, durante muchos años, ha emitido diversos reportes, informes y opiniones con relación al ciberterrorismo y el cibercrimen, considerando que son amenazas tanto para el mundo empresarial como para el social, donde la debilidad máxima es la desprotección de los usuarios y la falta de más información sobre estas.

Para el DCU, la lucha contra el ciberterrorismo empieza con la ciberseguridad, el mayor desafío para las compañías y líneas de defensa para las autoridades; pero ello no termina aquí. La lucha contra estas figuras requerirá una estrecha colaboración entre el gobierno y el sector

privado, esfuerzos continuados para mejorar la seguridad tecnológica, penas más severas para los ciberdelitos y un mayor financiamiento para los esfuerzos de aplicación de la ley para combatirlo, pues como ellos mismos resaltan, vivimos en un mundo interconectado que un ataque puede vulnerar desde el un municipio, hasta las más altas esferas de poder como el Pentágono de los EE. UU. Además, resaltan que los ciberterroristas son cada vez más sofisticados y organizados para tomar ventaja del mundo siempre en evolución y conectado.

2.3.4. *Symantec (Estados Unidos de Norteamérica)*

Para esta empresa de ciberseguridad fundada en 1982, hablar de ciberterrorismo es hablar de algo serio y que ha tomado mucho tiempo de investigación; así lo demuestra sus múltiples informes —como los ISRT y los *White Paper*— y contenidos en su blog oficial sobre el tema.

Para ellos, el combate contra el ciberterrorismo es un juego de defensa y ofensa, y consideran que la creación de instituciones como la cyber-OTAN traen consigo ventajas como la armonización de los códigos penales contra el ciberdelito; identificación e implementación de mejores prácticas y tecnologías para proteger la infraestructura de Internet; y la definición de protocolos y procedimientos estándar (McLean, 2009), pasos que se siguen llevando a cabo a la fecha. Aunque es un tema en el que han tenido presencia desde el 2002, época en donde aconsejaban la protección de las redes informáticas y las infraestructuras críticas, las industrias debían seguir desarrollando estrategias para combatirlo.

Así mismo, al hablar de ciberterrorismo, es sabido que la barrera de entrada es extremadamente baja, y al ser de bajo coste, rápido y efectivo, conseguir *neosoldados* es solo cuestión de tiempo, con entrenamiento de fácil acceso a través de un buscador (NICOLAS_POPP, 2010), herramientas y tecnologías que siguen disponibles al día de hoy, mismas que son comprobables con la presencia de grupos partidarios a ISIS en Twitter o YouTube en enero de 2015, luego de piratear las cuentas pertenecientes al gobierno de los EE.UU. (ISTR, 2016).

En líneas generales, SYMANTEC es claro y acepta al ciberterrorismo como una amenaza real, pero a la vez que convive con nosotros en la red real, utilizando elementos comunes para hacer efectiva su presencia. Si bien el ISRT 2017 no habla de ciberterrorismo, el informe del año anterior destaca el uso de Internet y las TIC por parte de los terroristas para generar amenazas cibernéticas y ampliar su mensaje, transformando estos en una herramienta radical y en un medio de comunicación y financiación de sus operaciones. Una amenaza que no para y que deja a la población y la industria vulnerable.

2.3.5. *Trend Micro (Japón)*

Con cerca de 30 años en el mercado de la seguridad y con 31 sedes en los cinco continentes, esta empresa fundada originalmente en Los Ángeles, California, se ha caracterizado por sus rápidas respuestas ante amenazas cibernéticas como el *ransomware*, y por brindar algunas soluciones gratuitas a usuarios. Esta experiencia brinda credibilidad cuando Trend Micro decide hablar sobre ciberterrorismo, una amenaza que ha calificado similar a la ciberdelincuencia, ya que los personajes que son parte de estas estructuras prefieren en el anonimato; permanecen en la Deep web y Dark web, donde evitan ser rastreados; difunden propaganda; e incluso, tienen sus propias herramientas y empresas dedicadas a estas actividades (KRAMER, 2016). Pero lo que los hace diferentes son sus tácticas de ataque, por ejemplo, las herramientas de mitigación DDoS. Los hackers pueden usar estas herramientas para ocultar el origen de los sitios web utilizados para comprar y vender kits de *exploits*, datos robados y otros contrabandos relacionados con el delito cibernético; mientras que los terroristas usarían esta herramienta como una forma de lanzar sitios web y blogs de propaganda, y posteriormente ocultar la IP alojada (BUDD, 2016). No podemos olvidar el uso del *spearphishing*, que en manos de los ciberterroristas podrían generar ataques más efectivos, como infiltrarse en los sistemas informáticos y moverse libremente dentro de los sistemas del proveedor del servicio, recopilar información valiosa sobre las medidas de seguridad implementadas en un área específica, e incluso, generar estafas para financiar sus movimientos (PAGANINI, 2015).

De igual forma, el ciberterrorismo también se encuentra en la web que conocemos y el mundo real. Utilizan redes sociales como Facebook o medios de mensajería como WhatsApp para la comunicación y la coordinación de acciones, y ejecutan ataques que afectan tanto al sector social como empresarial (KRAMER, 2016), ataques que incluso se pueden materializar en el espectro físico y generar disturbios y violencia contras personas o propiedades, accidentes aéreos, contaminación del agua, perdidas económicas, o solo generar miedo en la población (SWIMMER, 2010)

En conclusión, Trend Micro se une a la larga fila de organismos y empresas que aceptan la amenaza del ciberterrorismo y, por tanto, su existencia. A pesar de que en sus inicios se mostraran escépticos con su presencia en el mundo digital, hoy son conscientes que pueden desestabilizar la paz tanto en el entorno de la red como en el mundo real, además de mantenerse en constante estado evolutivo. Una amenaza de la que debemos entender sus metas y motivos.

2.4. Análisis y explicación de los principales expertos en el sector investigación, jurídico y ciberseguridad a nivel internacional en referencia a la peligrosidad de la figura del ciberterrorismo

Como parte de la estrategia argumentativa de esta investigación, se elaboraron tres entrevistas a tres reconocidos especialistas en el campo digital, de tres sectores diferentes. Es así como cada una de sus opiniones, en sus respectivos campos, brindaron una visión más amplia de los argumentos ya recolectados, he hicieron hincapié en puntos ya pronunciados y en nuevos esquemas que dejan más puntos por resolver, para dar así paso a futuras investigaciones en el campo tecnológico y de la ciberseguridad.

2.4.1. *Carlos Álvarez – Director of SSR Engagement de ICANN (Colombia - EE. UU.)*

Carlos Álvarez es un reconocido abogado que ha laborado tanto en la práctica del litigio como en la gerencia y el sector de seguridad en Internet, siendo uno de sus trabajos más reconocidos el que desempeña en ICANN, así como su colaboración con M^{3}AAWG. La entrevista se desenvolvió más en sus opiniones y experticia que en el campo de la corporación de Internet, pues esta última no guarda relación con los aspectos de la ciberseguridad y muchos menos en el campo del ciberterrorismo, sino que su función está guiada al campo de los nombres de dominio.

Álvarez define al ciberterrorismo como **«cualquier uso que se le da a recursos asociados a Internet como red global, de una manera que estos puedan afectar, de manera real, a la vida e integridad de la población de un país»**, brindando como ejemplo la detención del fluido eléctrico en una ciudad durante la temporada de invierno o suspendiendo el flujo de tráfico de intercambio de datos. A ello, Álvarez resaltó una nueva pregunta: ¿Un ataque de DDoS que impide el acceso a medios que usan las personas puede ser considerado ciberterrorismo?

La respuesta entabló una discusión muy interesante, pues hemos visto en la realidad que ante ataques DDoS se produce pánico en los usuarios e informes de todo tipo a través de Internet; pero esto no es suficiente para considerarlo ciberterrorismo. Como ejemplo de ello puede tomarse la caída de los *servers* de WhatsApp, en donde los usuarios solo deben tomar una vía alterna de comunicación como los viejos SMS y otro sistema como Messenger de Facebook.

Por otro lado, existen ataques a infraestructuras de servicios públicos que sí llegan a ser considerados como ciberterrorismo, como los ataques a Ucrania en el 2016, o los ataques a hidroeléctricas en EE. UU. en el mismo año; estos porque afectan a la población de una manera en la que su propia integridad está en juego, y no como en el caso anterior.

Cuando se le consultó a Álvarez sobre el acceso a la información de casos de ciberterrorismo y una posible obstaculización de este, afirmó que el

hecho que ciertas noticias sobre el caso no llegué al foco público se debe a dos factores: El primero, por tratarse de un tema de seguridad de Estado; y el segundo, porque no tuvo un gran impacto en la sociedad como se hubiera pensado. Esta respuesta tiene una raíz lógica, y es que, si bien el mundo se ha vuelto más tecnodependiente, y el ciberterrorismo sea una amenaza real, hay países más o menos dependientes de Internet y la tecnología, por lo que los efectos de un ciberataque no serán los mismos.

«Sí, el ciberterrorismo sí es una amenaza real, pero el impacto será mayor o menor dependiendo de muchos factores, como la relación del país y su acceso a la información», aclara.

Sobre la obstaculización de la información, alega que uno no puede prever la cantidad de escenarios que se puedan producir con relación a los ciberataques o el ciberterrorismo, que en muchas oportunidades la información no es debelada por encontrarse en una investigación en curso —como las que maneja la INTERPOL o EUROPOL—, o porque algún Estado —entendido como gobierno y no población—, bajo su decisión enteramente soberana, no desea dar información a su población sobre lo sucedido. Esto no debe considerarse obstaculización de información.

En cuanto al tema legislativo, Álvarez resalta que la lucha contra el ciberterrorismo y/o la ciberdelincuencia **«es mucho más que generar legislaciones»**. También deben tomarse en cuenta otros componentes como la implementación voluntaria de estándares técnicos como los definidos por la IETF: BCP-38[110]; BCP84[111]; *resort and resolvers*; así como actualizaciones y uniformización de legislaciones. Agrega que este es un trabajo de colaboración múltiple, en donde también ingresan las empresas; pero recalca que una legislación solo constituye el 5% de avance para resolver el problema, por lo que no es la solución a todo.

«Antes, el riesgo de estar expuesto a un ataque de Internet era mínimo. Ahora la tecnología nos ha hecho más vulnerables porque requerimos de más aplicaciones para más acciones», indica.

Finalmente, Álvarez dio una opinión acerca de la presencia de SL en Internet y cómo es posible que no haya podido darse de baja toda web relacionada al movimiento.

«Hay un error que es creer que los males nuestros son conocidos como propios. Hay que entender las diferencias culturales y entender que esperar de las empresas que brindar servicios de tecnología. No se puede esperar que todos entiendas cuales son nuestros problemas (…) Antes de preguntarnos porqué SL tiene esa web, debemos preguntarnos qué tanto entienden los ingenieros de qué es y quienes son SL».

[110] Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing.
[111] Ingress Filtering for Multihomed Networks.

Podríamos decir que este es un problema generalizado. Si bien SL cuenta con contenido en la web, la gran pregunta que el Derecho peruano ha buscado responderse es cómo es esto posible, no encaminándose a la propuesta de Álvarez que va más por el entendimiento de los proveedores de Internet. Para hacer frente ante este problema se resalta la existencia de mecanismos tales como el reporte de abuso, las vías legales, los tratados de asistencia legal mutua, las cartas rogatorias o la intervención de las cancillerías de los países en donde se aloja el contenido de SL.

Y si aún quedan dudas del porque la presencia en Internet de SL tiene menos impacto que la de ISIS, se deben a que este último tiene mayor presencia en los medios en general. Es por eso por lo que, aplicándose el mismo principio, los equipos de ingenieros tienen más información de este grupo que del otro, teniendo a su vez más contacto con los ataques y amenazas que generan.

Como conclusión a esta entrevista cabe destacar una vez más la presencia real del ciberterrorismo, así como el impacto de sus acciones que no serán iguales en cada país, dependiendo siempre del nivel de uso que se le dé a las tecnologías e Internet. En el caso de Perú, si bien todavía no llegamos a la interconectividad máxima, esta es una de las metas para el año 2021, según la Agenda Digital del país. Finalmente, está claro que el avance legislativo es una buena propuesta que dará chance a mayores avances de defensa, pero si solo nos quedamos en lo legislativo, no será productivo para luchar contra esta amenaza. Se hace necesario la implementación de estándares técnicos como los definidos por la IETF, entre otros, así como un trabajo de concientización para un mayor conocimiento de las amenazas que puedan producir los grupos terroristas tradicionales en el ciberespacio, así como amenazas ciberterroristas.

2.4.2. *Lorenzo Martínez – CTO (Chief Technical Officer) de Securizame (España)*

Hoy por hoy, Lorenzo Martínez es considerado uno de los mejores *hackers* de Europa y a nivel internacional. *Speaker* de larga data, ha sido parte de importantes proyectos como el Observatorio Iberoamericano de Protección de Datos (actualidad) y la Declaración de México D.F., hacia la implantación de garantías para la privacidad en los tratamientos de Big Data (2014). La entrevista se direccionó por el lado de la ciberseguridad como estructura Estatal y sus opiniones del trabajo del Derecho en este mundo tecnológico.

Martínez empieza esta entrevista dando su opinión sobre la consulta que se le hizo sobre el trabajo del Derecho en el campo tecnológico y de la ciberseguridad, resaltó que era una cuestión imposible y que era como ponerle puertas a un campo, una de sus frases famosas. Explicaba que, cuando se buscan hacer leyes, estas se hacen por país y todas tienen como finalidad regular Internet, cuando Internet no puede ser regulado y su ejercicio —guiado por la práctica tradicionalista— muchas veces es

injusto, pues el mismo hecho con la misma casuística puede ser considerado delito en un país y no en otro; o en donde la pena sobre un mismo hecho sea diferente en diferentes lugares. Destaca en esta observación el problema del salto de servidores y cuestiona al Derecho tradicional para descubrir bajo qué Ley juzgarían a una persona que ataca a un país desde un segundo país, utilizando servidores simultáneos de un tercer y cuarto país. Él mismo pregunta dónde se cometió el delito.

Quiere dejar en claro que, si bien se requieren de abogados especializados y que entiendan el mundo de las tecnologías e Internet, esa falta de conocimiento y experticia ha hecho muchas veces que el Derecho cierre el paso al trabajo de *hackers* y de la ciberseguridad.
«Muchas veces la adquisición y utilización de ciertas evidencias no sirven por cuestiones de privacidad y datos personales, siendo estas más importante que llegar a la verdad (…) Existe una sobreprotección de la persona que incluso se pueden invalidar pruebas por no tener permiso para constatar su navegación; o por acceder a información que no se puede acceder», agrega.

Con relación a esto último, que puede traer gran debate con el Derecho, Martínez afirma que las autorizaciones judiciales, así como el exceso de burocratización pueden entorpecer los peritajes informáticos.

«En España, los cuerpos del Estado están tan abarrotados de casos, que cogen aquellos casos graves y se ponen (a trabajar) con ello. El tiempo puede hacer que las pruebas no sirvan, que la información se haya sobrescrito, borrado o no esté accesible. El exceso de burocratización termina siendo perjudicial», aclara.

Y es que la investigación en el campo digital no discrepa de la investigación en un ambiente físico, donde las pruebas están contra el tiempo y su deterioro es amiga del reloj. Es por ello por lo que muchas empresas optan por el informe pericial privado, en donde solo se cuenta con la autorización de los dueños y un contrato con el perito forense digital, transformándose así en un perito de parte y no un perito judicial.

Continuando con el punto de la entrevista, se consultó a Martínez sobre su definición de ciberterrorismo, a lo que este la precisa como **«la utilización de TIC relacionadas/conectadas a Internet para robar, modificar o para inutilizar otros sistemas distintos causando perjuicio a otra persona, por respuesta a algo o por cuestiones monetarias».** Agrega que **«vulnerar el correcto funcionamiento de infraestructuras críticas puede ser considerado ciberterrorismo»**. Así mismo, se le comentó que, en el año 2009, un cuerpo de la PNP[112] presentó un proyecto al Congreso de la República del Perú para regular el ciberterrorismo, recibiendo una respuesta negativa y alegando que no se pensaba regular ni debatir sobre figuras inexistente, algo que puede ser refutado en este tiempo, y que el mismo Martínez considera que, más que regular sobre figuras inexistentes,

[112] La identidad de los oficiales no se develará por cuestiones de protección y privacidad.

la realidad pudo ser que no pensaban trabajar sobre figuras que no entienden.

Añade que, si bien en España hay propuestas y avances legislativos para luchar contra el ciberterrorismo, no se cuenta con un apoyo técnico, por lo que muchas de sus legislaciones son burdas e inexplicables, como la popular Ley de Cookies. Así mismo, considera que una legislación nacional no es suficiente, y que una norma internacional es lo más ideal para la lucha contra el ciberterrorismo, una norma que cuente con múltiples actores y que demuestre el verdadero interés del Estado de romper la brecha digital y no entorpecerla.

Como conclusión a esta entrevista se pueden destacar varios puntos. En primera instancia —y como se ha mencionado en múltiples ocasiones—, el Derecho tradicional y su metodología no es compatible con las necesidades del mundo moderno y con las gestiones de ciberseguridad, donde el factor tiempo sigue siendo un jugador indispensable en el tablero. En segunda instancia, si bien se confirma que el ciberterrorismo es una amenaza real, el paso legislativo único no es suficiente, recomendándose un trabajo universal y, a futuro, la propuesta de una legislación única. Finalmente, y en tercera instancia, la ley solo será beneficiosa si se cuenta con el cuerpo jurídico y técnico capacitado, por lo que queda demostrado —indirectamente— que se requiere de un arduo trabajo de capacitación en múltiples sectores.

2.4.3. *Julio Téllez – Investigador titular en el Instituto de Investigaciones Jurídicas de la UNAM (México)*

El nombre de Julio Téllez Valdés se pronuncia cada vez que de Derecho y tecnologías se habla. Con una alta producción, es quizás el investigador jurídico más respetado a nivel LATAM y uno de los más destacados en el mundo legal. Ha ocupado puestos importantes tanto en organizaciones nacionales e internacionales, y es constantemente consultado cuando se desea alguna referencia en cuanto al Derecho tecnológico. En este caso, la entrevista tomó un rumbo dirigido a la investigación y al fundamento crítico de las amenazas en el ciberespacio.

Como los otros entrevistados, Téllez tiene su propia opinión sobre ciberterrorismo, definiéndolo como **«un riesgo real de seguridad nacional»**; un concepto diferente al de sus primeras investigaciones en los años 80, ya que, como destaca el investigador, el ciberterrorismo se mostraba más como una problemática a nivel de seguridad interna (pública), y que hoy ha ganado más importancia al ser ahora una figura en el enfoque de seguridad internacional.

Sin embargo, Téllez considera que este sigue siendo un tema muy delicado de tratar, y que va más allá de las amenazas y de los ataques que se puedan producir.

«A veces, algunos Estados, utilizan el terrorismo para poder ejercer un control sobre la ciudadanía. A veces, no pueden regular sobre algo a lo que echan mano para controlar a la población», explica.

El ciberterrorismo no discrepa de cualquier ciberdelito, puesta que también emplean herramientas que brindan beneficios propios o ajenos; pero, lo que podrían desligarlo de este último grupo son sus intereses, más ligados a ideales que a elementos pecuniarios, y que va en contra de los intereses e integridad de las personas. Es por ello por lo que debe trabajarse en políticas públicas, en legislación nacional y, a gran escala, en legislación internacional.

Igualmente, aclara que el ciberterrorismo y el terrorismo está ligado al ciberespionaje, y que esta es una práctica divisada en todos los entornos, pudiendo llevar a múltiples cuestiones. Y si bien ya existe un pronunciamiento de la ONU con relación al ciberespionaje, todavía queda un retraso por parte de los legisladores al no considerar la información como un bien susceptible de ser apoderado.

«Si los cambios no son posibles para hacer frente a la nueva delincuencia, deben darse nuevos conceptos, generarse nuevas figuras y tipificarse. Mientras no estén considerados en el ámbito penal, no pueden ser considerados delitos, con lo que deben generarse leyes acordes a la realidad», agrega.

Sobre este punto, Téllez tiene una clara visión, y explica que, si se tiene una ley actualizada, se debe buscar capacitar a las autoridades para que den cumplimiento de esta y tengan los elementos necesarios para hacer cumplimiento de sus funciones. Aquí no cabe solo la presencia de abogados litigantes; también de la policía, quienes deberá perseguir a los delincuentes que trabajen bajo la nueva modalidad estipulada en la norma —previas capacitaciones—; y a los jueces y fiscales, quienes deberán estar actualizados y tener conciencia de lo que enfrentan, con nuevas normas y nuevas figuras típicas.

Dos puntos más se plasmaron en la entrevista: El Derecho Penal del Enemigo y el Global Trends de la CIA. Con relación al primero, Téllez señala que la cuestión de esta respetable teoría es que fue engendrada con el tema de los DD. HH. de fondo, punto donde los mismos delincuentes se han beneficiado; esto hace que haya una coalición inevitable, pero que no deje de pensarse que el terrorismo es un mal que debe de ser segregado de la sociedad por el daño que le causa al Estado como ciudadanía, no como gobierno. Sobre el segundo punto, menciona que, en EE. UU., a raíz del atentado del 11 de septiembre, se dieron cuenta de la vulnerabilidad a la que estaban expuesto; sin embargo, es un país que tiene los fondos suficientes para combatir a la amenaza terroristas y ciberterrorista, por lo que reclutan equipos tanto para la defensa como para nuevo reclutamiento, ya no van por el factor independiente sino por el factor de beneficio grupal. Resalta una frase del 43° presidente estadounidense George W. Bush: **«En el futuro habrá guerras que se verán y no se verán»**.

Téllez termina esta entrevista señalando que el problema del terrorismo es que no se sabe nunca donde va a suceder, y si bien existen el Convenio de Budapest —que aún tiene temáticas por resolver— y el Estatuto de Roma, esto no es suficiente para combatir un problema como el ciberterrorismo. Se hace necesaria la presencia de una nueva legislación, tanto a nivel nacional como internacional, y con este último aplicar el principio de la extraterritorialidad.

Como conclusión a esta entrevista se rescatan las recomendaciones de empezar por una legislación nacional para luego dar paso a propuestas de índole internacional. Por otro lado, se hace presente la recomendación de actualización legislativa, un trabajo que no se ha concretado en el Perú y que, como se ha podido percibir, constituye una amenaza mayor que propio ciberterrorismo, el cual, una vez más, ha quedado demostrada su existencia. Finalmente, el trabajo en la lucha contra el ciberterrorismo no es solamente jurídico. La presencia del cuerpo policial, el elemento judicial y —aunque no fuera mencionada— el cuerpo técnico tecnológico, se hacen de vital importancia como parte de una estrategia de defensa ante una amenaza que el Estado peruano se niega a ver, pero que existe, tanto en el espacio como en el ciberespacio.

2.5. El ciberterrorismo como problema para la seguridad ciudadana en nuestro país y su importancia dentro de la agenda política

Uno de los puntos que no se ha discutido con profundidad, pero que es importante incorporar por la realidad que vive el Perú es la inseguridad ciudadana, problemática que ha sumergido a la ciudadanía en una convivencia con diversos delitos como el robo a bancos —tanto dentro como fuera de las instalaciones—, secuestros, extorsiones, marcas[113], asesinatos, entre otros. Y si bien se habló de seguridad ciudadana en la primera tesis sobre ciberterrorismo elaborada por el autor en el año 2014, es el *OAS-First Cyber Security Symposium* (2016) donde se pudo comprobar que la seguridad ciudadana no es ajena a los avances tecnológicos de la sociedad y los peligros que se generan en Internet. Colombia es uno de los países que ha visto esta realidad y la lucha contra el ciberdelito se encuentra dentro de su plan de seguridad ciudadana.

En el Perú, para hacer frente al problema de la inseguridad ciudadana, se crea el **SISTEMA NACIONAL DE SEGURIDAD CIUDADANA** (2003), el mismo que se constituye en el máximo organismo a nivel nacional para lograr la plena integración entre el Estado y la sociedad civil para alcanzar óptimos niveles de seguridad ciudadana en el marco del fortalecimiento de un cultura de paz; cuya **MISIÓN** es la de **«formular, conducir y evaluar las políticas de seguridad ciudadana a nivel nacional con la participación activa de los organismos del Estado, Gobiernos locales y la comunidad organizada con la finalidad de garantizar el pleno ejercicio de los derechos consagrados en la Constitución Política del Perú, así como la convivencia pacífica»** (SANTIVÁÑEZ M., 2013).

[113] Entiéndase por ***marcas*** a aquellos criminales que asaltan a los clientes de bancos luego de haberles hecho un seguimiento profundo y asaltarlos el día que realizan una gran transacción de dinero.

Del mismo modo, esta norma legal establece por **OBJETO** el **«proteger el libre ejercicio de los derechos y libertades, garantizar la seguridad, paz, tranquilidad, el cumplimiento y respeto de las garantías individuales y sociales a nivel nacional. Comprende a las personas naturales y jurídicas, sin excepción, que conforman la Nación Peruana»** (SANTIVÁÑEZ M., 2013).

A pesar de contar con este sistema, la práctica parece no mostrar resultados de su efectividad; y en la percepción ciudadana, tampoco. Para dar un mayor enfoque de la problemática en el Perú, el 2015, el Barómetro de las Américas del Proyecto de Opinión Pública de América Latina (LAPOP) ubicó al país en el primer lugar de inseguridad en la región, con un 30.6% de encuestados que aseguraban haber sido víctimas de la delincuencia. A ello sumemos que solo el estudio toma como referencia el peligro físico y no virtual; este último —como ya se ha señalado— terminará generando pérdidas de más de US$ 4,782M (cuatro mil setecientos ochenta y dos y 00/100 millones de dólares americanos) para finales de 2017. Misma respuesta —en relación al ciberespacio— se encuentra en las Estadísticas de Seguridad Ciudadana del INEI[114], que informan que en el 2016 se registraron un total de 16 412 denuncias por ciberdelitos en las dependencias policiales, pero continúan manteniéndolos en la estructura de delitos de hurto agravado, a pesar de la nueva ley de ciberdelitos ya no les da esta clasificación; así como la evaluación del plan de seguridad nacional del CONASEC, que no solo no incluye una evaluación de la peligrosidad de los ciberdelitos, tampoco recibe una actualización desde el periodo enero-julio de 2016[115], demostrando una vez más el poco interés por parte del Estado y sus autoridades de corregir la problemática delincuencial, así como su estructura organizacional en el ámbito digital.

La defectuosa lucha contra la inseguridad ciudadana ha generado ventajas en el hampa y una sensación de intranquilidad en la población peruana. Esto se debe a que, a pesar de contar con una norma que permita hacerle frente— en palabras del especialista en seguridad ciudadana, Cnel. PNP (R) Juan José M. Santiváñez Marín—, **«no existe una política de Estado en materia de seguridad ciudadana»**. Como remarca el especialista en sus múltiples entrevistas, **«cada gobierno y gobernante considera hacer lo mejor para hacer frente a la inseguridad existente, en donde el ciudadano común es víctima permanente de la delincuencia común y organizada; donde la violencia familiar y la violencia contra la mujer va en aumento cada día y no se realizan programas sociales para atender a las víctimas ni mucho menos a los menores y jóvenes en riesgo social; sin llegar a entender, que el problema de la inseguridad ciudadana no solo debe ser visto por el Poder Judicial, Ministerio Público, Policía Nacional o Ministerio de Justicia, sino que éste es un problema más grande».**

Como punto final, si bien existió grandes intenciones con la formulación de una nueva normativa en ciberdelitos para el Perú, la información recabada para este punto ha demostrado que nunca se estableció un plan de trabajo que generara conexión entre esta legislación y el plan nacional de seguridad ciudadana. Esto podría suponer que no existió una recomendación aparente o un comando técnico

[114] Toda la información de los estudios estadísticos a la fecha se encuentra en su apartado web: https://www.inei.gob.pe/biblioteca-virtual/boletines/estadisticas-de-seguridad-ciudadana/1/
[115] Toda la información se encuentra en su sitio web: http://conasec.mininter.gob.pe/

especializado que recomendara dicha vinculación. Sin embargo, muy a pesar de ello, si el Estado peruano no puede responder ante la peligrosidad latente en el país en el sector físico, es evidente que no podrá hacerlo en el mundo digital, y muchos menos contra una amenaza como el ciberterrorismo.

2.6. El ciberterrorismo como cuestionamiento ante su ausencia en la ley de ciberdelitos del Perú

En este punto de la investigación no hay duda de que el ciberterrorismo es una de las mayores amenazas a nivel global, y que son muchos los países que vienen preparándose de una u otra manera, ya sea por medio de una modificatoria a su legislación con relación a los ciberdelitos; sea con la propuesta de una nueva legislación a trabajar o la formación de nuevos equipos de respuesta ante incidentes cibernéticos, como alianzas con los países mejor preparados. Sea cual fuera el caso, el Perú no ha ingresado en esta lista de trabajo global, y muchos menos ha tomado una de estas iniciativas como ejemplo.

Si no empezamos a dar los primeros pasos, si la amenaza ciberterrorista se manifiesta de más formas, cuando haya concentrado puntos que todavía no ha terminado de desarrollar, será mucho más difícil combatirla legalmente, pues se habrán generado conductas que no podrán ser sancionadas, y cuando se busque sancionarlas, los ciberterroristas ya habrán cambiado su modalidad.

Hoy por hoy, uno de los mayores problemas en el Perú es la poca visión que se tiene sobre ciberseguridad y normativa relacionada. Se pensó en un instante que cuando la DINI luchaba por tener la gestión de la seguridad de Internet en el Perú se hablaría de ciberterrorismo y la necesidad de combatirlo, pero brilló por su ausencia. Ahora con la Ley N°30618 (2017) promulgada, el Perú perdió no solo la oportunidad de ingresar al Convenio de Budapest; además, la posibilidad de dar paso a un verdadero cambio legislativo y a una preparación en materia de seguridad digital que ya maneja la región, y en donde nos llevan años de ventaja.

Queda claro que legislar la figura del ciberterrorismo no es prioridad para la nación y sus poderes político, mucho menos la prioridad del Derecho o de alguna organización vinculante presentar un estudio e iniciativa para dar paso a la discusión. Las comisiones que se han formado —por ejemplo, en el CAL—, para hablar de temas relacionados al Derecho y TIC están dormidas en eventos y discusiones a las que especialistas en la región le encontraron solución hace más de una década. Tenemos años de atraso, se ve en todas las figuras, y si cuestionamos nuestra estructura en raíz del ciberterrorismo, esta solo confirma que seguimos siendo vulnerables y no hacemos nada para cambiarlo. No estamos preparados, esa es la verdad.

2.7. La importancia de la ciberseguridad en el ámbito de la seguridad ciudadana como herramientas para combatir la figura del ciberterrorismo

Si entendemos que el objeto de la seguridad ciudadana es el proteger el libre ejercicio de los derechos y libertades, garantizar la seguridad, paz, tranquilidad,

el cumplimiento y respeto de las garantías individuales y sociales a nivel nacional, esto no solo debe limitarse al campo físico, sino que agrega en su contexto —indirectamente— al mundo digital. Esto puede entenderse ya que, aun ingresando a Internet, cuya posesión no es de la jurisdicción de un país, la calidad nacional no se pierde, pero se ignora.

A estas alturas de la investigación, y luego de entender la importancia de la seguridad ciudadana para la convivencia social y armónica de una población, debe recomendarse incluir dentro del plan nacional un punto donde se plantee una estrategia para combatir los ciberdelitos y, a futuro, el ciberterrorismo; no necesariamente como un plan de ciberdefensa nacional, pero sí como una estrategia para defender al ciudadano de a pie, que ciertas veces se ve más afectado que las propias instituciones.

Si podemos tomar un ejemplo de países que velan por la seguridad ciudadana en el ámbito digital, EE. UU. firmó el **ACTA DE PATRIOTISMO** (2001), documento en donde las principales empresas de comunicaciones se comprometían y garantizaban al Gobierno de su país —en caso de riesgo de seguridad nacional—, el acceso a datos que se hayan sido subidos a Internet o cualquier tipo de información que permita capturar a algún criminal (PABLO & DE AZUMENDI, 2013). Y si bien esto puede constituir una violación a los datos personales de cualquier usuario que haya subido información a la red, debemos recordar que muchas veces la sobreprotección de la persona puede invalidar pruebas o entorpecer procesos (MARTÍNEZ, 2017), por lo que este tipo de acciones deben ser vistas como acciones en defensa de los intereses de la nación.

Otro ejemplo es España, país que siguiera los pasos de EE. UU., instaurando el conocido **MANDO CONJUNTO** para hacer frente a los ciberataques; y desde el año 2013 la INTERPOL, EUROPOL y la OTAN vienen hablando de un sistema de ciberdefensa en la lucha contra la criminalidad (PABLO & DE AZUMENDI, 2013). Y así podemos seguir sumando otras iniciativas de varios países de la región como Colombia, que mantiene alianzas estratégicas con Canadá y Estonia (2016), países con altos estándares en la temática de la ciberdefensa y la lucha contra el cibercrimen, para preparar a los responsables de la defensa de su país y también contrarrestar en alianza los ataques a infraestructuras críticas.

El ciberterrorismo coloca una valla muy alta en el tema defensivo y de respuesta para los países a nivel mundial. El Estado peruano debe comprender que no solo importa la defensa de la integridad de sus ciudadanos en el espectro físico y tangible, también es importante la protección en el ámbito del ciberespacio y sus universos. Si bien la ley de ciberdelitos busca tener esa función, si no se complementa con el plan nacional de seguridad ciudadana, seguirá fracasando como lo ha hecho desde su promulgación. Del éxito de ese trabajo conjunto depende también que la futura inclusión como delito de la figura del ciberterrorismo tenga éxito.

Como punto conclusivo debemos recordar que estos esfuerzos deben darse de manera progresiva, pero también rápida. El mundo interconectado nos sumerge en diversas paradojas que muchas veces los legisladores no comprender, por creer

que ambas caras de la misma moneda funcionan de similar manera. Un claro ejemplo son las modalidades de ataque, que muchas veces no requieren de programas especializados para ingresar a un sistema de algún país, solo conocer los servidores y sus vulnerabilidades (ALONSO, 2013); y como ya se ha señalado en este estudio, el no conocer dichas vulnerabilidades, es solo una parte de nuestra gran debilidad. Contamos con poco tiempo para generar un plan de respuesta ante el ciberterrorismo y para enlazar nuestra lucha contra este y la ciberdelincuencia con la seguridad ciudadana.

3. Marco conceptual

3.1. Conceptos relacionados al problema

3.1.1. *Ciberterrorismo*

Actividad en donde, por medio de las TIC e Internet se busca generar terror o miedo generalizado en una población, clase dirigente o gobierno, causando con ello una violación a la libre voluntad de las personas. De acuerdo con la nueva visión de seguridad, se descarta las acciones movidas solo por fines políticos y/o religiosos para considerarlas terrorismo.

3.1.2. *Ciberdelito*

Término genérico que hace referencia a la actividad delictiva llevada a cabo mediante equipos informáticos o a través de Internet. El ciberdelito puede hacer uso de diferentes métodos y herramientas, como el *phishing*, los virus, *spyware*, *ransomware* o la ingeniería social, normalmente con el objetivo de robar información personal o de realizar actividades fraudulentas (AVAST, 2017).

3.1.3. *Ciberseguridad*

Protección de activos de información, a través del tratamiento de amenazas que ponen en riesgo la información que es procesada, almacenada y transportada por los sistemas de información que se encuentran interconectados (ISACA, 2016).

3.1.4. *Ciberguerra*

El uso de la tecnología para interrumpir las actividades de un estado u organización, especialmente el ataque deliberado de los sistemas de información con fines estratégicos o militares (OXFORD DICTIONARY, 2017). Conjunto de acciones llevadas por un Estado para penetrar en los ordenadores o en las redes de otro país, con la finalidad de causar perjuicio o alteración (CLARKE, 2010).

La ciberguerra también hace referencia al desplazamiento del conflicto al ciberespacio; aunque muchas veces Bruce Schneier, gurú en ciberseguridad, explicara que es difícil definir un concepto tan amplio

como la ciberguerra por lo imposible de saber cómo queda el ciberespacio luego del encuentro bélico.

3.2. Marco legal

3.2.1. *La regulación establecida por el legislador peruano para referirse a la figura de ciberterrorismo*

En el Perú, la regulación referida a los ciberdelitos sufre su primera modificatoria al promulgarse la Ley N°30096 – Ley de Delitos Informáticos en el Perú; que deroga la Ley N°27309 y sus artículos expresados en el Código Penal de ese entonces (Artículos 207°-A; 207°-B; 207°-C y 208°); para luego, ante la coyuntura y los excesivos errores normativos en la modificatoria, se planteara y promulgara una segunda modificatoria, la Ley N°30171; siendo todo este proceso fruto de los Proyectos de Ley 034/2011-CR; 307/2011-CR y 1136/2011-CR, proyectos que desde sus inicios mostraban el escaso entendimiento por parte de nuestros legisladores sobre Internet, la sociedad y los ciberdelitos. Por otro lado, esta nueva ley no ha integrado a sus filas uno de los principales delitos a nivel internacional como es la figura del ciberterrorismo, figura que países como Estados Unidos se ha preparado desde hace más de 14 años.

En el Código Penal Peruano, el delito de terrorismo ha sufrido una evolución luego de su derogación en el año 1992[116]. Con la Ley N°26926, del 21 de febrero de 1998, se agregan nuevos puntos contra el delito de terrorismo, señalando al genocidio, la desaparición forzada, la tortura y la cooperación profesional en la perpetración del delito de terrorismo como sancionables de este mismo delito. No obstante, a pesar de la nueva figura que se ha desarrollado con los años, no se ha presentado una nueva modificación en donde se incluya en esta lista a la figura del ciberterrorismo, dejando vulnerable tanto al legislador peruano para juzgar a este tipo de cibercriminal —puesto que su accionar no se encuentra dentro del tipo penal—, como a la sociedad misma, desprotegida ante este hecho delictivo, y como hemos visto, el ciberterrorismo no se limita a la apología, también centra sus habilidades en el ataque y la captación de miembros. Las normas quedan desactualizadas y no existe proporción entre realidad y seguridad.

3.2.2. *La figura del ciberterrorismo según el Derecho comparado*

La figura del ciberterrorismo se presenta, a nivel internacional, como un mal tan dañino como el terrorismo simple, con la misma finalidad, pero en donde no se busca poner en riesgo —en primer plano— la integridad física del elemento terrorista, pero sí la capacidad cognoscitiva de la sociedad,

[116] Capitulo derogado por el Artículo 22° del Decreto Ley N°25475 (1992), ley que establece la penalidad para los delitos de terrorismo y los procedimientos para la investigación, la instrucción y el juicio. Abarca los antiguos Artículos 319° al 322°.

implantando el miedo; así como los medios digitales, sistemas de defensa de gobiernos y a los gobiernos mismos. Es decir, el ciberterrorismo afecta más que a un sistema y puede ser tan peligroso como un explosivo en un edificio, haciendo remembranza de la época terrorista vivida en la década de los ochentas y noventas.

Por el momento, son muchos los países que trabajan en una normativa actual relacionada a la figura del ciberterrorismo, más aún en una manera de combatirlo. Estados Unidos de Norteamérica invierte millones de dólares en ello, incluso ha trabajado en la creación de cibersoldados listos para la ciberguerra[117]. Por otro lado, países como Colombia[118] y Panamá[119] vienen trabajando desde tiempo en la búsqueda de la penalización del ciberterrorismo; así como China, país que desde mayo de 2017 efectúa una ley contra el ciberterrorismo[120]; pero esto no es un trabajo únicamente de abogados —como siempre lo ha manejado la casta política nacional—. Si no se trabaja con los especialistas correctos, los esfuerzos serán inútiles. Estos países buscan formas más acertadas de poner sancionar a los criminales que ejecuten diversos tipos de ciberdelitos, pero aún no tienen una respuesta si nos referimos a la figura del ciberterrorismo. Gran avance se ha dado al aceptarlo como una amenaza, sea social o corporativa. Ese debería ser también nuestro primer foco, aceptar a la figura del ciberterrorismo como una amenaza global y real.

Por lo que se puede apreciar, el mundo no es ajeno a la evolución del crimen, mucho menos los gobiernos que buscan actualizarse. Los juristas peruanos no pueden darle la espalda a la realidad que cada vez se hace más tecnológica en el planeta. Deben generase generar las armas tanto legales como tecnológicas para combatir a los ciberdelincuentes y los cibercrímenes.

3.3. Otros marcos

3.3.1. *Las teorías que ayudan a explicar la importancia de regular la figura de ciberterrorismo en nuestra normativa nacional*

Tener una sola teoría como base para explicar la importancia del Derecho dentro del ámbito de los ciberdelitos; más aún, como explicación a la

[117] INI, Federico. **Óp. Cit.**

[118] REDACCIÓN EL ESPECTADOR (2010). **«Gobierno de Colombia busca penalizar el Ciberterrorismo»**. 2017, del portal El Espectador, sección *Nacional*. Sitio web: https://www.elespectador.com/noticias/nacional/articulo-228922-gobierno-buscara-penalizar-ciberterrorismo

[119] REDACCIÓN SEGURIDAD INFORMÁTICA (2012). **«Panamá: Buscan penalizar intrusiones ilegales en sitios de internet»**. 2017, de Seguridad Digital [Fuente: Sdpnoticias]. Sitio web: http://seguinfo.wordpress.com/2012/03/10/panama-buscan-penalizar-intrusiones-ilegales-en-sitios-de-internet

[120] Cfr. REDACCIÓN EC (2017). **«China efectuará una ley contra el ciberterrorismo y piratería desde el jueves»**. Del portal El Comercio, sección *Tecnología*. Sitio web: https://elcomercio.pe/tecnologia/tecnologia/china-efectuara-ley-ciberterrorismo-pirateria-jueves-426836

importancia de la penalización de la figura del ciberterrorismo, es también ceñirla a una limitación. Existen muchas teorías que nos podrían ayudar a explicar la importancia de penalizar una figura como el ciberterrorismo, algunas más dinámicas que otras; es por ello por lo que se ha analizado cada teoría y se ha visto conveniente explicar las que se consideran importantes para el presente plan de Tesis.

En primera instancia, se plantea la elección del **IUS NATURALISMO** por sobre el **IUS POSITIVISMO**, teniendo sustento en que este último plantea que el Derecho es un conjunto de normas dictadas por los seres humanos, a través del Estado, mediante un procedimiento formalmente válido, con la intención o voluntad de someter la conducta humana al orden disciplinario acatando las mencionadas normas, afirmándonos que su finalidad está guiada a la gestación de normas con ubicación geográfica pre-establecida; es decir, en una parte específica del planeta, algo que no puede concebirse en Internet, al ser este de dominio global. Efecto contrario se encuentra en el **IUS NATURALISMO**, teoría ética que posee un enfoque filosófico del Derecho, el mismo que postula la existencia de derechos del hombre fundados en la naturaleza humana, universales, anteriores y superiores —o independiente— al ordenamiento jurídico positivo y al derecho fundado en la costumbre o derecho consuetudinario. Esto permitirá que la norma que se plantee para combatir y considerar como delito la figura del ciberterrorismo; si bien, en primer lugar, se centraría de manera nacional, no tenga un límite regido por una ubicación geográfica. Se refuerza este punto agregando que la figura del ciberterrorismo no requiere de la presencia física para su actuación, lo que dificultaría no solo la norma a elegir para la sanción, sino en parte, como ha sucedido en ciertas ocasiones, identificar al responsable de la conducta delictiva.

En segunda instancia, la elección de la **SOCIOLOGÍA DEL DERECHO** ayuda a la fundamentación del marco teórico. También llamada **SOCIOLOGÍA JURÍDICA**, es aquella disciplina que estudia los problemas, las implicancias y todo aquello concerniente a las relaciones entre la sociedad y el Derecho. A diferencia de la teoría del Derecho y de la filosofía política, su principal problema y objeto de estudio es el que la eficacia del Derecho, que es lo que se necesita para combatir la figura del ciberterrorismo.

Los ciberdelitos, al igual que cualquier otro delito existente y regulado, tiene un sinfín de víctimas establecidas, siendo la principal víctima de la sociedad, pero no cualquier sociedad. En este caso hablamos de una sociedad existente en el ambiente físico y una sociedad existente en el ciberespacio, fruto de la sociedad física, ambas con la necesidad de ser reguladas de manera efectiva para impedir que los ciberdelitos sigan esparciendo su accionar delictivo y afectando a los partícipes de la sociedad.

Si bien en estos casos nos centramos en teorías que nos permiten ahondar más en el ámbito real de los ciberdelitos, en especial, de la importancia que

tiene la figura del ciberterrorismo, la presente Tesis busca ayudar más al legislador peruano en profundizar el conocimiento legal para generar una necesaria y efectiva regulación.

4. Hipótesis

4.1. Hipótesis general

La figura del ciberterrorismo constituye alta peligrosidad para nuestra nación, especialmente porque este no ha sido considerado como un delito en nuestra legislación.

4.2. Hipótesis específicas

- El desarrollo de las TIC otorga elementos que facilitan la expansión de la figura del ciberterrorismo en nuestra nación.
- La falta de una legislación que tipifique la figura del ciberterrorismo genera un vacío legal aprovechado por los cibercriminales para ejecutar acciones terroristas en Internet.

4.3. Variables e indicadores

HIPÓTESIS GENERAL

- **Variable Independiente (X)**: *Ciberterrorismo como peligro nacional*
- **Indicadores:**
  X1: Inminente amenaza a la estructura nacional

- **Variable Dependiente (Y):** *Inexistencia en la normativa nacional*
- **Indicadores:**
  Y1: Normas desactualizadas
  Y2: Normas no acordes a la realidad nacional
  Y3: Normas no acorde a la realidad internacional

I HIPÓTESIS ESPECÍFICA

- **Variable Independiente (X):** *Desarrollo de las TIC*
- **Indicadores:**
  X1: Tecnología sin límites
  X2: Tecnología al alcance de todos

- **Variable Dependiente (Y):** *Ventaja para el ciberterrorismo*
- **Indicadores:**
  Y1: Sin límites ni ubicación forzosa para un ataque
  Y2: Sin límites para la expansión de su ideología

II HIPÓTESIS ESPECÍFICA
❖ **Variable Independiente (X):** *Falta de legislación que tipifique la figura del ciberterrorismo* ❖ **Indicadores:** X1: Ciberterrorismo no es reconocido como delito en el Perú. ❖ **Variable Dependiente (Y):** *Vacíos legales aprovechados por criminales* ❖ **Indicadores:** Y1: No hay manera legal de enfrentar al ciberterrorismo Y2: Ventajas para los ciberterroristas

CAPÍTULO III
MÉTODO

1. Tipo de investigación

Para esta investigación se empleó el **MÉTODO INDUCTIVO** que consiste en recolectar información mediante sucesiva observación para establecer ley mediante la generalización, siendo la principal fuente de información Internet, el campo en donde se guarda la mayoría del conocimiento utilizado y el lugar que sirve como campo de ejercicio para los ciberterroristas.

Con relación al segundo aspecto, se analizó y comprobó las actividades que venían realizando los terroristas en Internet, centradas en captación a través de redes sociales y generación de contenido en páginas web, todo ello con el fin de demostrar que la presencia del ciberterrorismo lleva tiempo en el Perú y es momento de hablar de legislación.

De igual forma, se optó por elaborar una encuesta dirigida a la población de diferentes estratos sociales, edades y profesiones, y así saber si la población en general tiene conocimiento de esta amenaza y/o que opiniones tiene sobre esta.

Como complemento se empleó el **MÉTODO DE ANÁLISIS** que consiste en ejecutar una operación intelectual que permite considerar por separado un todo. Es decir, cada hipótesis específica necesitaba ser comprobada antes de conectarse entre sí y, finalmente, con la hipótesis principal, para demostrar que lo dicho en esta investigación está en lo correcto, y cada uno de los complementos utilizados, la consulta a los expertos y los informes analizados terminaron por darle es sustento y la fortaleza que este trabajo buscaba.

2. Diseño de la investigación

Para la investigación se utilizó un diseño **NO EXPERIMENTAL** del tipo **TRANSVERSAL**; es decir, la recolección de datos producida en un momento —en este caso, durante transcurso mayor a los cinco años— y que ayudaron a analizar las variables representadas en la figura de la hipótesis. La encuesta producida no deja de ser una metodología adicional para la recolección de datos. Los encuestados no son objeto de experimento y su opinión solo busca se contrastada con la realidad, mas no generar debate con los datos recolectados.

3. Estrategia de la prueba de hipótesis

Si bien este aspecto del trabajo de investigación está más guiado a investigaciones de campo que de materias jurídicas, se tomó en cuenta para analizar dos aspectos importantes que se tuvieron en mente: **La percepción global inicial** de la hipótesis, que nos demuestra que, para el Perú, existe la posibilidad de la no existencia de la figura del ciberterrorismo; y **la percepción del investigador**, que es demostrar que la

existencia, peligrosidad y amenaza que representa la figura del ciberterrorismo. Es así como tenemos el siguiente cuadro explicativo.

HIPÓTESIS	EXPLICACIÓN
Hipótesis nula (H0)	La figura del ciberterrorismo no es una amenaza real en el mundo y menos una figura de alta peligrosidad para el Perú, por lo que no se hace necesaria la creación de una ley especial.
Hipótesis alternativa (H1)	La figura del ciberterrorismo constituye alta peligrosidad para nuestra nación, especialmente porque este no ha sido considerado como un delito en nuestra legislación.

La **hipótesis nula (H0)** es la hipótesis que se busca rechazar con esta investigación centrada en la recolección de datos. La **hipótesis alternativa (H1)**, en la mayoría de los casos —como el de esta investigación— es la tesis por la que se parte y que se busca demostrar.

4. Variables

El bloque de variable se dividió en cuatro, analizando de esa manera la hipótesis general, hipótesis específicas y la idea primaria que se tenía del por qué realizar las encuestas y en qué ayudaría su resultado.

HIPÓTESIS GENERAL	EXPLICACIÓN
Variable independiente	El ciberterrorismo como una amenaza a la nación y al interés del Estado.
Variable dependiente	Falta de legislación con relación al tema y de equipos de respuesta inmediata ante la amenaza.
Variable intermedia	El ciberterrorismo no es considerado un delito en el Perú.

I HIPÓTESIS ESPECÍFICA	EXPLICACIÓN
Variable independiente	El desarrollo de las TIC al alcance de todos.
Variable dependiente	Ventajas para el accionar del ciberterrorismo.
Variable intermedia	El acceso que generan las TIC con Internet no tiene límites, ni espacio ni tiempo, con lo que se tiene un gran campo de ataque.

II HIPÓTESIS ESPECÍFICA	EXPLICACIÓN
Variable independiente	Falta de legislación que tipifique la figura del ciberterrorismo en el Perú.
Variable dependiente	Vacíos legales aprovechados por criminales.
Variable intermedia	Mientras no exista una norma, no se puede juzgar a una persona por ciberterrorismo en el Perú, con lo que su accionar sigue estando protegido.

PROCESO DE ENCUESTAS	EXPLICACIÓN
Variable independiente	El conocimiento de la población ayuda a saber que tan informados están del ciberterrorismo y sus peligros.
Variable dependiente	Saber con cuanta seriedad está enfrentando este problema la población nacional.
Variable intermedia	Las repuestas están condicionadas al conocimiento previo que tengas las personas, por lo que tampoco puede ser tomada como una respuesta total, solo como datos.

5. Población

Para el desarrollo de la investigación no ingresa el factor población al tratarse de una recolección de datos. No obstante, se ideó una estrategia para estar informado sobre el conocimiento que tenía la población sobre esta materia, lo que serviría como una nueva base de datos.

Se realizaron 103 encuestas en total para el siguiente estudio estadístico, las que fueron completadas por personas de diversas edades y estratos sociales. La finalidad era demostrar la poca información que maneja la población sobre la figura del ciberterrorismo y sus metodologías, así como el mucho o poco interés con este tema y afines. Se clasificaron en tres grupos:

- Jóvenes (entre 18 y 29 años).
- Adultos (entre 30 y 59 años).
- Adultos mayores (de 60 a más años).

6. Muestra

6.1. Muestra cualitativa

Representada en el material de estudio recopilador para la presente investigación, contando con un aproximado de 150 elementos recolectados y revisados en el transcurso de cinco años, siendo el menor número el de bibliografía relacionada a investigaciones de terrorismo, ciberdelitos y ciberdelincuencia, con un aproximado de 11 títulos hasta la fecha. Así mismo, la mayor cantidad de producción presente es de material extranjero y bajo licencias CC, con lo que queda descartado el interés nacional por producción relacionada a esta materia y afines, siendo esta la principal debilidad. La producción mayoritaria la hacen los *journals* especializados, informes y páginas web.

6.2. Muestra cuantitativa

Este muestreo se refleja en la encuesta, en donde se analiza una población para saber si esta tiene conocimiento o ha escuchado hablar sobre la figura del

ciberterrorismo y, de ser así, plasmar sus opiniones en la investigación. El resultado pasará a ser parte de la muestra cualitativa.

CLASIFICACIÓN DE GRUPOS	POBLACIÓN
Jóvenes (entre 18 y 29 años)	53 personas
Adultos (entre 30 y 59 años)	48 personas
Adultos mayores (de 60 a más años)	02 personas
TOTAL (Población)	**103 personas**

7. Técnicas de investigación

7.1. Instrumentos y/o fuentes de recolección de datos

Esta tesis está basada enteramente en **muestras cualitativas**, por lo que la recolección de los datos provino de libros en materia de derecho, terrorismo, ciberseguridad y ciberdelitos; así como *journals* especializados que hablan de temas relacionados a la tecnología, Internet y ciberterrorismo; investigaciones realizadas por empresas de ciberseguridad a nivel mundial; informes de las principales organizaciones internacionales, en las que se recolecta su opinión y visión sobre el ciberterrorismo; entrevista a expertos en la materia; publicaciones en diarios, revistas y cualquier medio de comunicación que tratara la temática del ciberterrorismo. Entonces, se utilizaron los siguientes datos:

- Análisis documental (libros, *journals*, informes especializados, vídeos).
- Entrevista asistémica o libre a expertos en la materia.
- Encuestas personales.

Podemos considerar a la encuesta desarrollada como un instrumento de recolección de datos, pero buscaba datos en específico, no en conglomerado en general. Sin embargo, es mi deber informar que, aun sin realizar la encuesta, el resultado final de comprobación de hipótesis no varía, ya que solo se buscaba tener información del conocimiento que tiene la población sobre la figura del ciberterrorismo.

7.2. Validación de los instrumentos por juicio de expertos

El siguiente cuadro representa el objetivo por el cual se recurrió a expertos para ayudar en la validez de la investigación.

PROCESO DE VALIDACIÓN	EXPLICACIÓN
Objetivo de la validación	▪ Verificar la veracidad de la información obtenida en durante los cinco años que duró la recolección de datos. ▪ Comparar si lo establecido en las hipótesis contrasta con la opinión de los expertos.

	▪ Conocer la opinión de los expertos con relación al ciberterrorismo, sus opiniones y si guardan la misma opinión que lo establecido en los informes presentados por las organizaciones internacionales, las empresas privadas y por el investigador de la tesis.
Expertos	▪ Tres expertos con más de 10 años de experiencia (comprobados) en el campo de las TIC e Internet, provenientes de tres áreas diferentes: Derecho, seguridad y organización internacional. ▪ Cada uno de los expertos ha tenido participación en los foros más importantes de su materia, así como conferencias y publicaciones, sin dejar la experiencia en el campo técnico y la investigación.
Modo de validación	▪ Se realizó una entrevista con preguntas centradas en su materia, experiencias profesionales y de investigación, todas centradas en el ciberterrorismo y su peligrosidad. ▪ Se buscó que las preguntas no inducirán a una respuesta determinada, sino que cada experto brinde su respuesta y su visión sobre el tema.

7.3. Técnicas de procesamiento de los datos

7.3.1. *Cualitativo*

Para el sistema de recolección de datos se siguió el siguiente parámetro:

1º. Libros relacionados a las materias del Derecho, la ciberseguridad y la tecnología, con una antigüedad no mayor a los 05 años desde su publicación o actualización. En ciertos casos se utilizaron libros de mayor antigüedad para hacer una comparación de visiones, realidades y evolución de ciertos conceptos y criterios.
2º. Legislación nacional que parta desde los proyectos de Ley en materia relacionada a ciberdelitos, ciberseguridad y afines. Entre los documentos destacan la Ley N°27309; los proyectos de Ley N°034/2011-CR, N°307/2011-CR y N°1136/2011-CR.; Ley N°30096; Ley N°30171, y la Resolución Directoral Nº1695-2005-DIRGEN/EMG-08AGO2005 que crea la División de Delitos de Alta Tecnología de la DIRINCRI, entidad encargada de combatir la

ciberdelincuencia en el Perú. También se consultó el código penal vigente y la constitución política del Perú de 1993.

3º. Legislación nacional en materia de terrorismo. También se consultó el código penal vigente y la constitución política del Perú de 1993.
4º. Legislación internacional en materia de ciberdelitos, ciberseguridad y afines, que no se encuentren vigentes, elaboradas tanto por países como por convenios.
5º. *Journals* especializados en diferentes idiomas que traten la problemática del ciberterrorismo, terrorismo, ciberseguridad, ciberderecho y afines, con una antigüedad no menor a los 05 años desde el día de su publicación. De preferencia, se buscó las últimas publicaciones del año en curso y del año anterior.
6º. Páginas web y vídeos en canales de YouTube, consultando siempre la procedencia y veracidad del contenido. De preferencia, se buscó en páginas y canales en instituciones periodísticas conocidas y de renombre internacional como CNN y BBC. Toda publicación no debía tener una antigüedad menor a los 05 años. En ciertos casos, se obvió esta opción para tener información comparativa.
7º. Informes especializados en materia de seguridad y afines, elaborados por las principales organizaciones internacionales como la OEA, el BID, la ONU o la OTAN; así como de empresas dedicadas al sector de la ciberseguridad como ESET, Trend Micro o Kaspersky, de fechas más recientes, y descargados de sus propias webs institucionales y corporativas, respectivamente.
8º. Entrevistas a tres especialistas en materias relacionadas al Derecho y la seguridad, con años de experiencia en el campo y prestigio internacional. Se propuso una primera lista de más de 20 candidatos y se suprimió a los 03 más importantes en la actualidad. Para la selección se hizo una búsqueda exhaustiva de su perfil profesional, publicaciones y conferencias elaboradas y participación en foros importantes.
9º. Encuesta a 103 personas de diversos sectores socioculturales para conocer su perspectiva sobre el terrorismo, ciberterrorismo y ciberdelitos en nuestro país. Las entrevistas se realizaron de manera personas en el plazo de dos semanas.

7.3.2. *Sobre la encuesta*

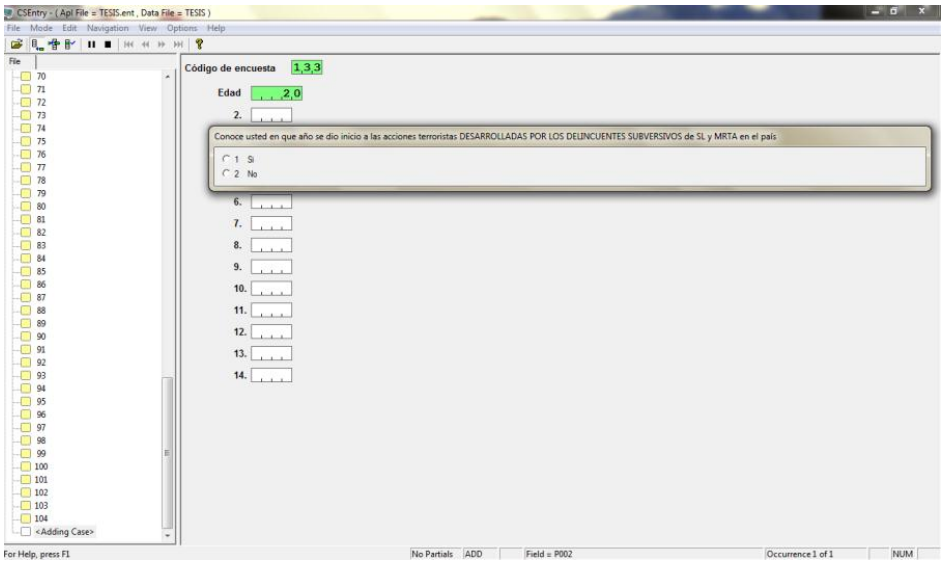
Siguiendo los parámetros del presente trabajo, para la realización del estudio estadístico y las preguntas a responder, se llevó a cabo la utilización de tres programas para no solo generar las preguntas, sino además una MASCARA, que no es otra cosa que los resultados de las encuestas realizadas en el estudio, y las gráficas correspondientes para hacer más efectivo el entendimiento del resultado.

- **Programa N°01: CSPRO 5.0**

  Es un programa de uso libre cuya función principal es crear máscaras para la introducción de datos (DATA ENTRY). Es decir, crea una

encuesta virtual en la que se pueden introducir los datos de cada encuesta de manera más sencilla.

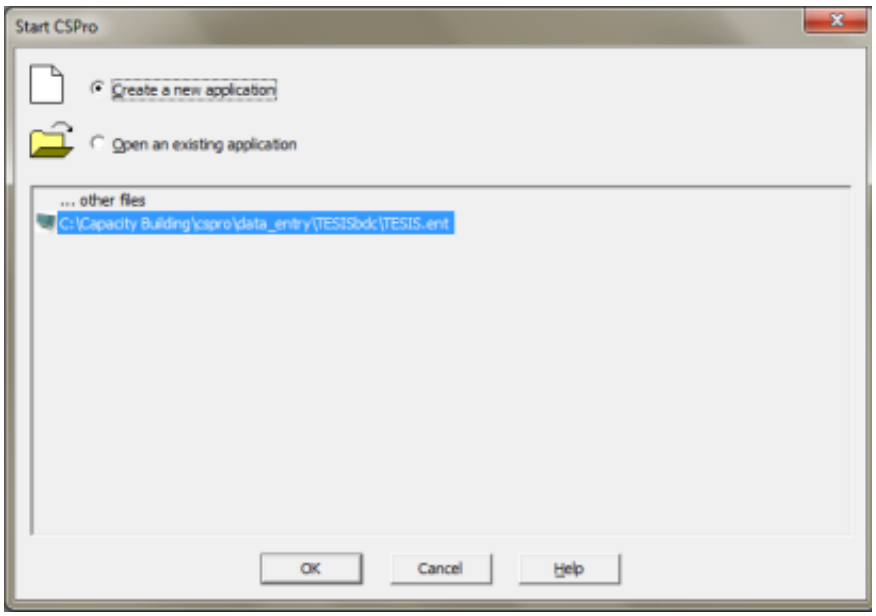
- Vista del programa a trabajar:



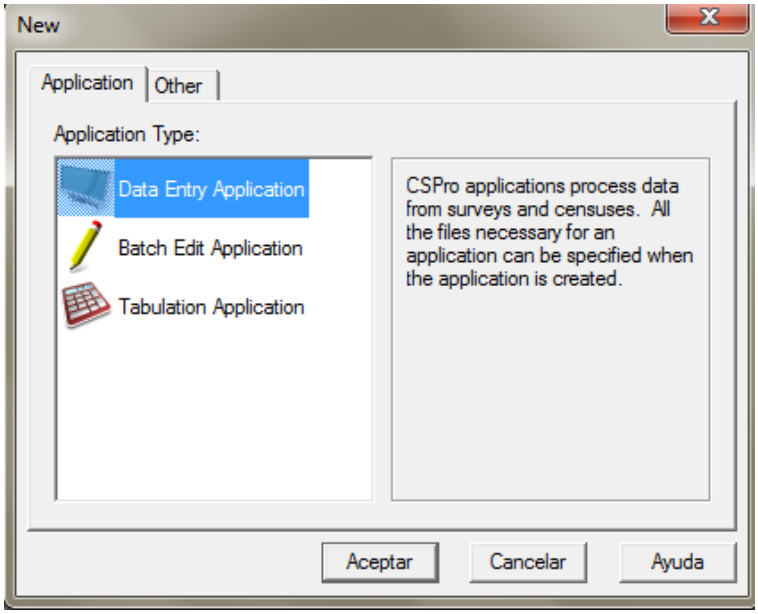
- Manera de Utilización:

a. Creación de máscara:

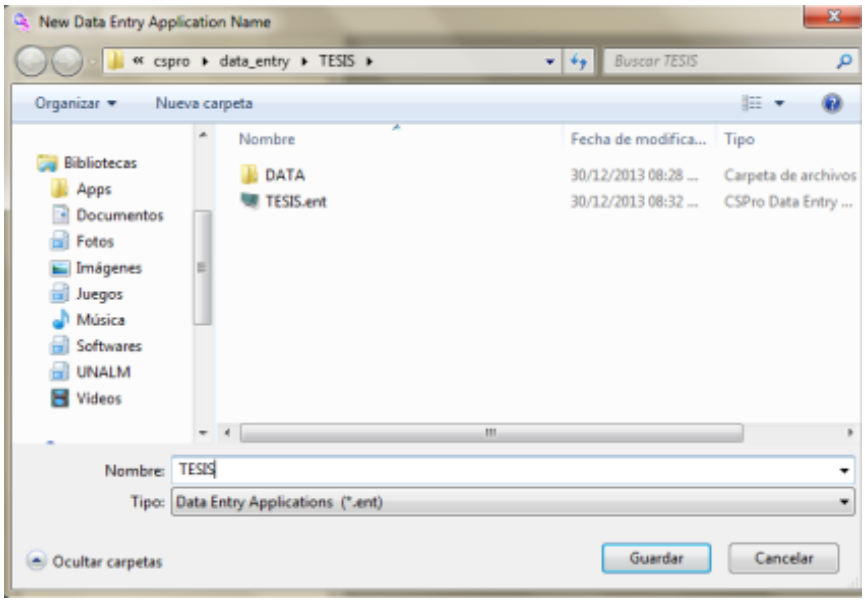
1. Crea una aplicación.



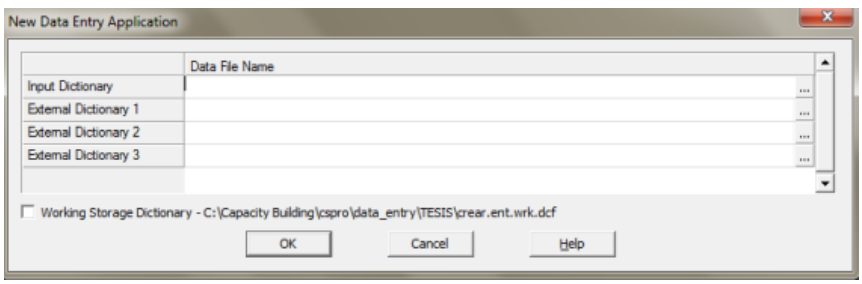
2. Crear una DATA ENTRY APPLICATION.



3. Poner nombre a la aplicación.

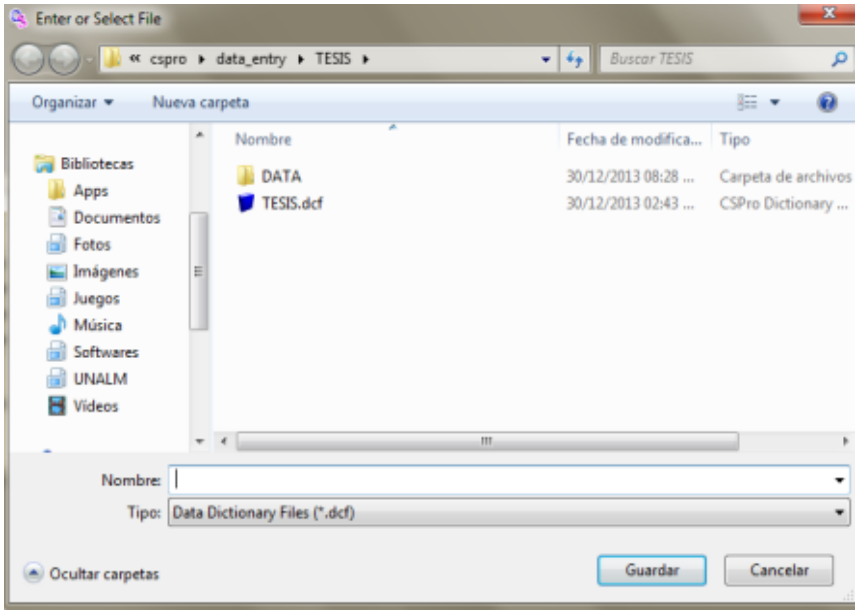


4. Creas el diccionario[121] de la aplicación.



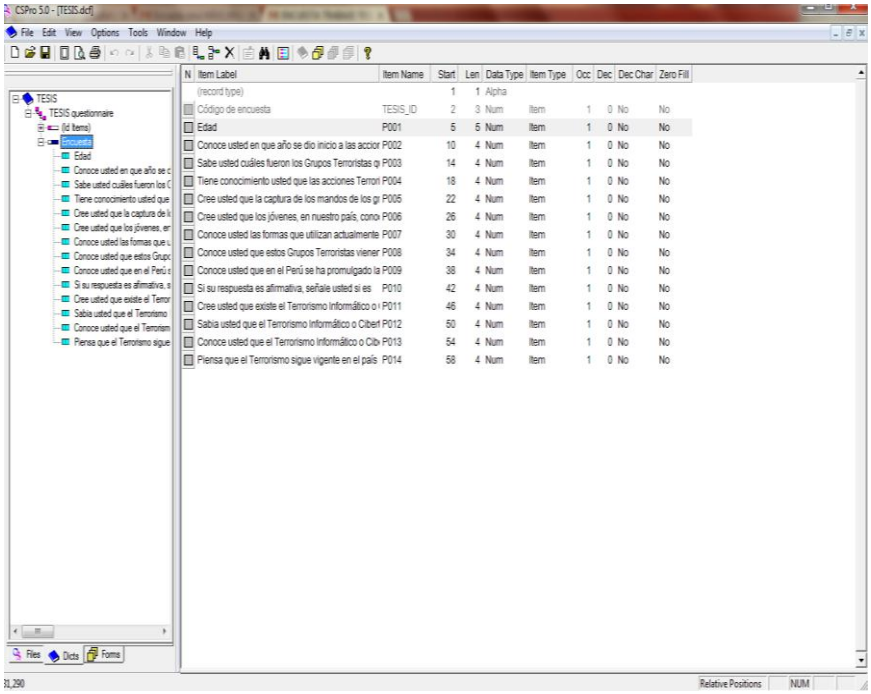
[121] Conjunto de preguntas y alternativas que tiene cada una.

5. Creas nombre para el diccionario.

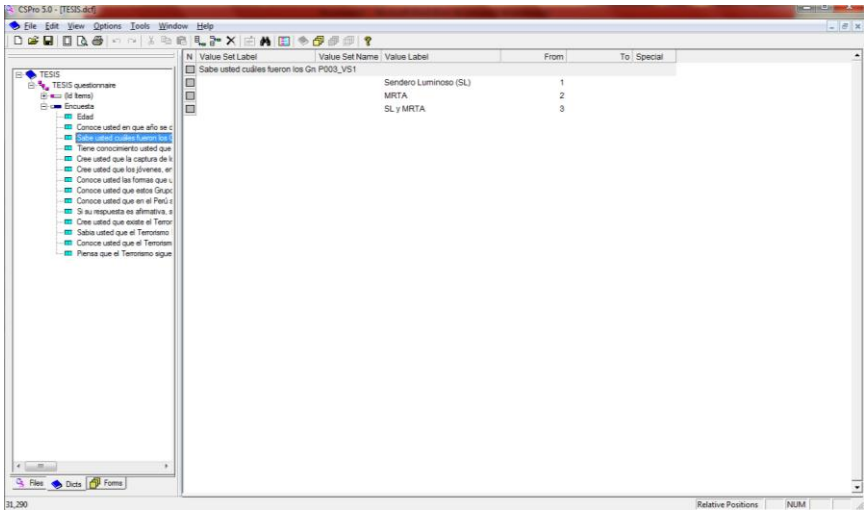


6. Una vez creado todo, comienzas a crear la encuesta.

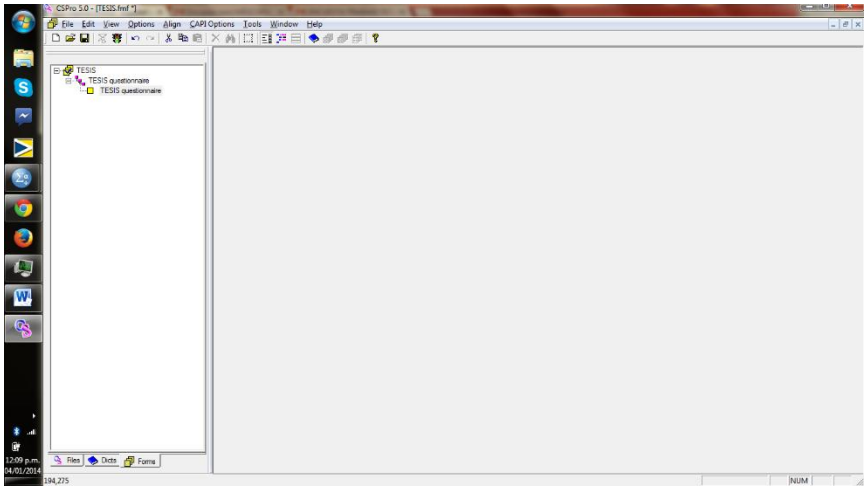
- Comienzas con el ID: es el código individual de cada encuesta (ID ITEMS).
- Luego siguen todas las preguntas de la encuesta. (ENCUESTA). Al crear las preguntas tienes que tener en cuenta las características de cada una.
- El código de la pregunta (ITEM NAME), la extensión de la respuesta (LEN) y el tipo de variable (DATA) que en estos casos todos son numéricas.



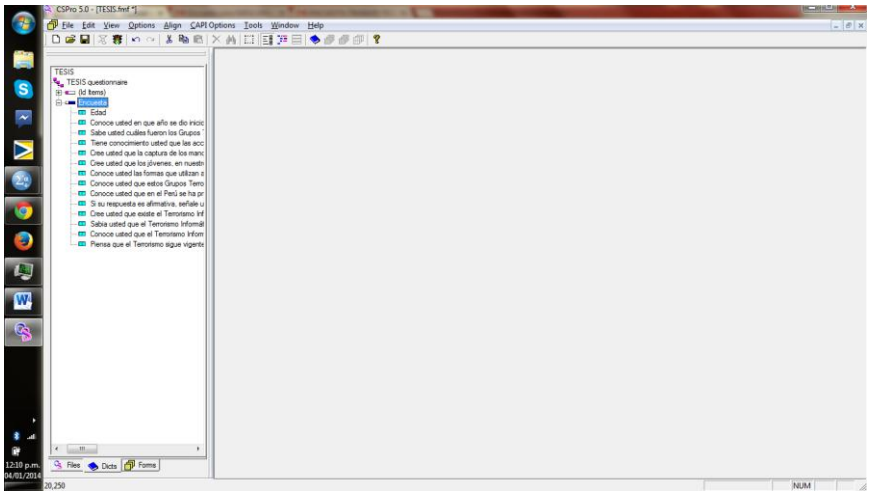
7. Ahora se crea las etiquetas de cada pregunta, según corresponda. Al crearlas, debe darse un número de opción.



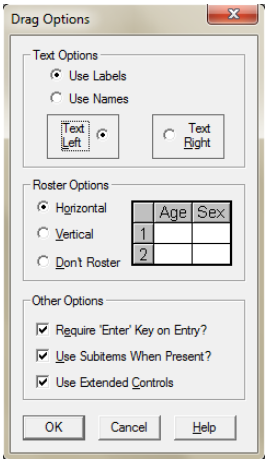
8. Una vez terminado el diccionario se procede a crear la forma o el aspecto que tendrá la máscara.



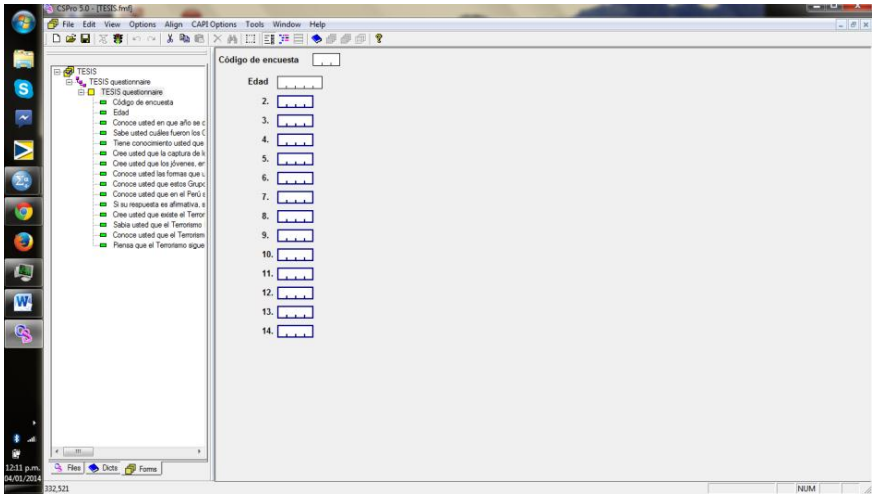
- Se arrastra el archivo encuesta a la pantalla.



- Marcar USE EXTENDER CONTROLS que permite la aparición del menú de opciones en el momento de que este introduciendo los datos de las encuestas.



- Editas de la forma que quieres las preguntas.

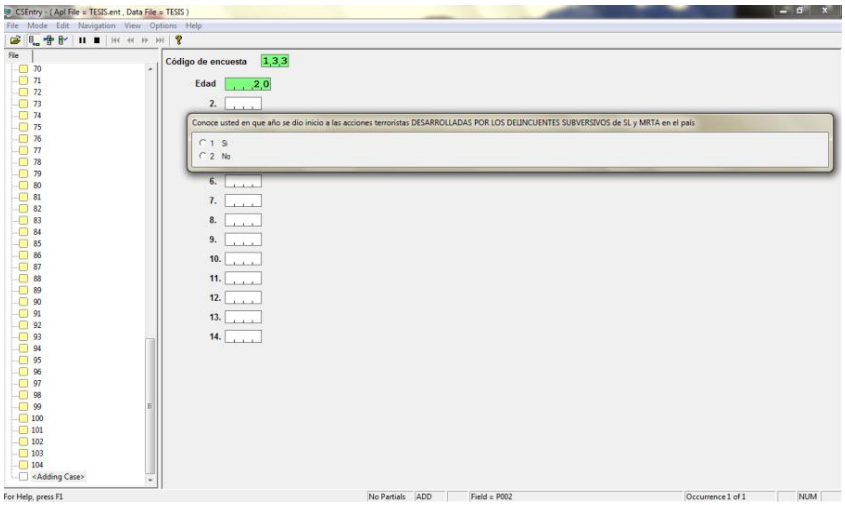


9. Una vez terminada la encuesta se corre el programa (CTRL+R).

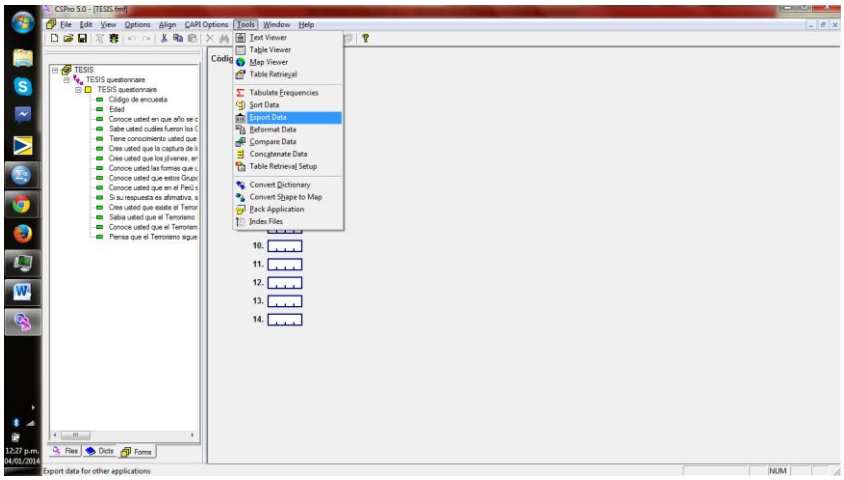
10. Se crea un nombre para la base de datos.

11. Se introduce un nombre al operador (cualquiera).

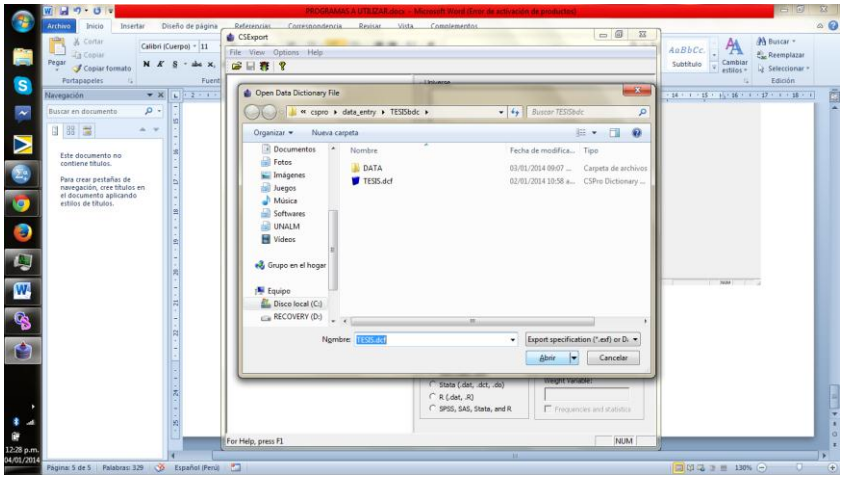
12. Se introducen los datos de cada encuesta bien sea marcando la opción en el panel o introduciendo el número de la opción seleccionada (al finalizar, se coloca aceptar).



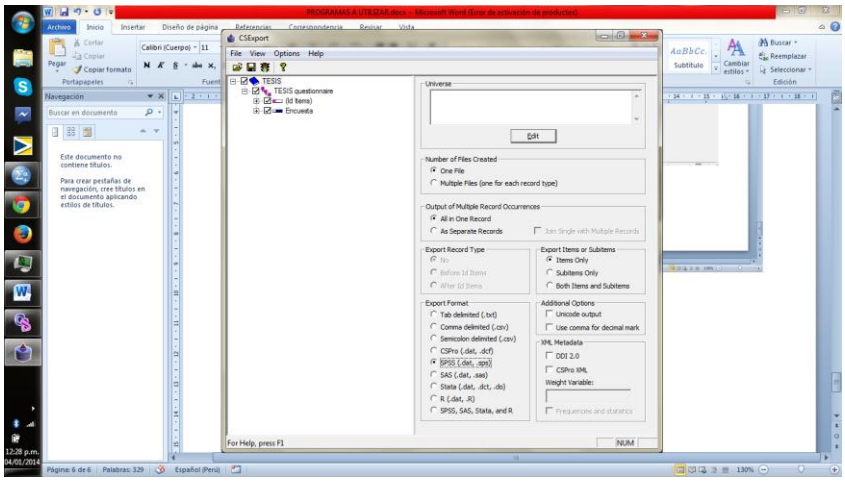
13. Una vez introducido todos los datos y verificado que estén correctos se crea la BASE DE DATOS.



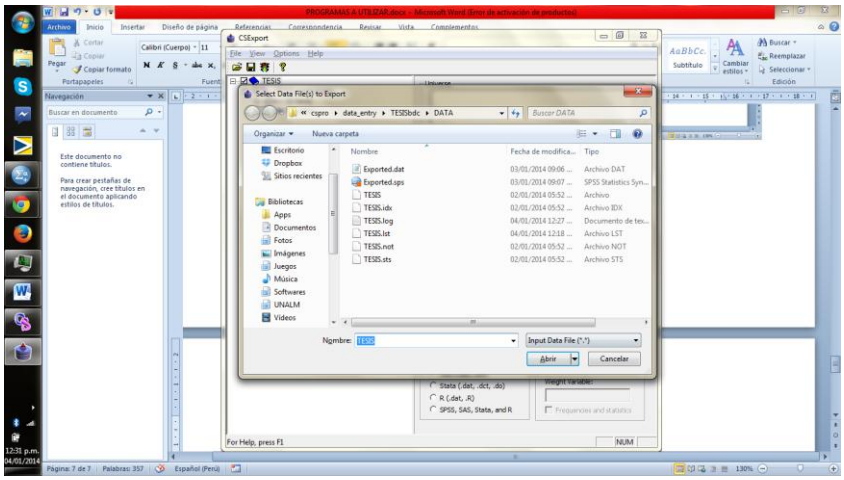
14. Selecciona el diccionario.



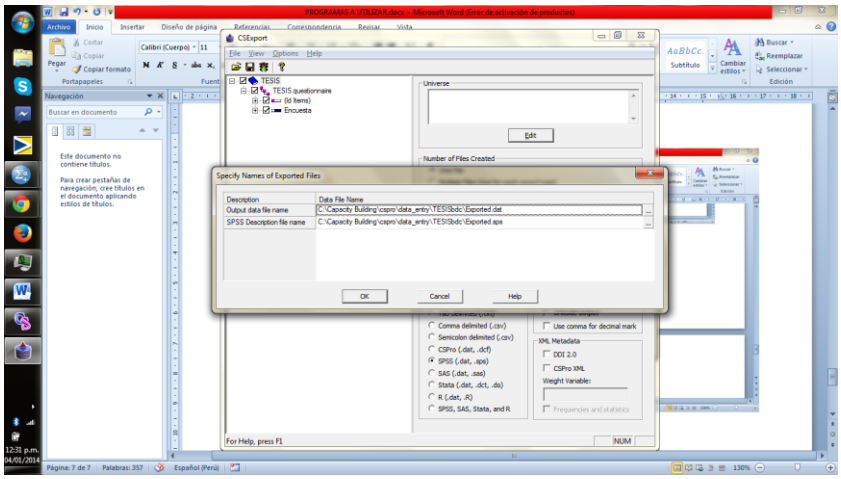
15. Seleccionas todos los capítulos del diccionario y la opción SPSS (.dat, .sps).



16. Luego se corre el programa (CTRL + R) y se selecciona la base de datos.



17. Se selecciona en donde se guardará el archivo SPSS de extensión .sps (nombre del archivo en este caso Exported.sps).



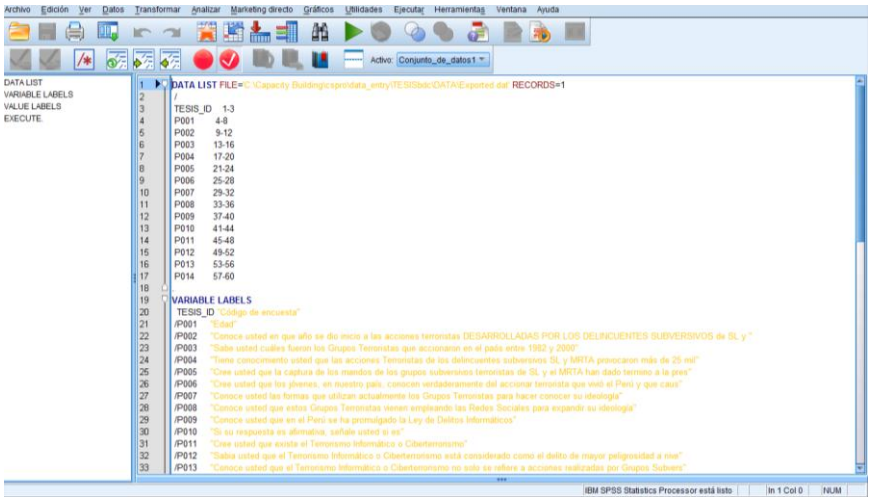
- **Programa N°02: SPSS 20**

  También conocido como *Statistical Package for the Social Sciences*, es el programa estadístico de mayor uso por sus menús simples, el formato de sus presentaciones y su simplicidad para el manejo de bases de datos.

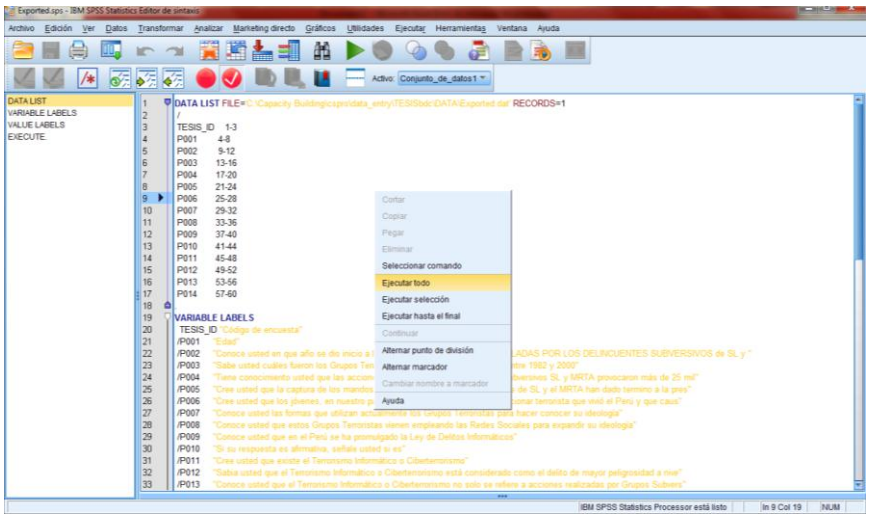
  El SPSS le facilita crear un archivo de datos en una forma estructurada y también organizar una base de datos que puede ser analizada con diversas técnicas estadísticas.

  Se utilizó el SPSS solo para generar las tablas estadísticas. El procedimiento fue el siguiente:

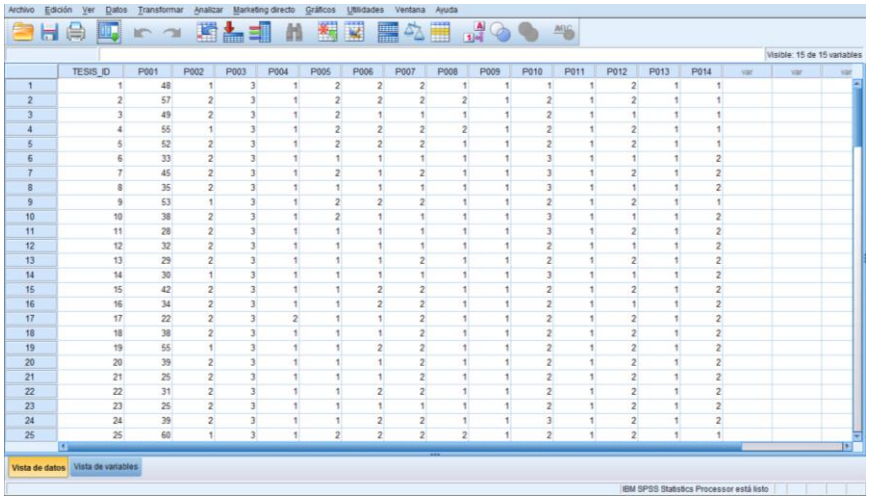
  1. Obtenidos los datos en el archivo Exported.sps se procede a abrirlo.



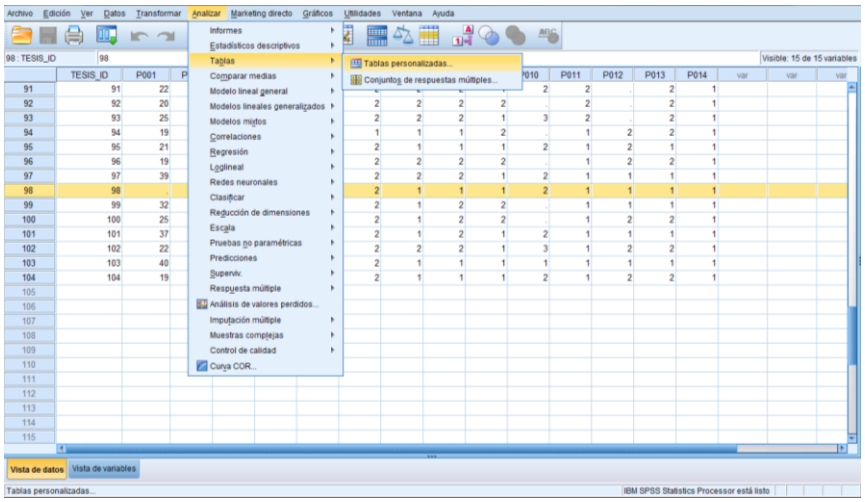
Y ejecutar toda la sentencia (anticlick/ejecutar todo).

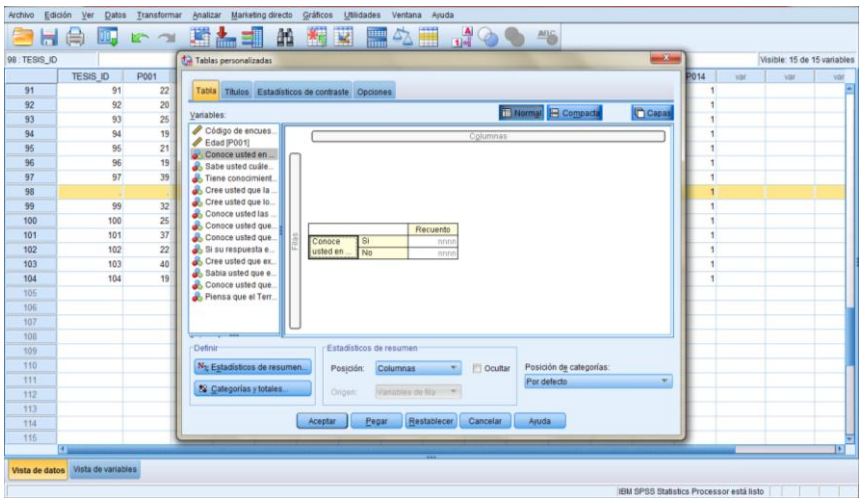


2. Creándose la base de datos, esta se debe guardar.



3. Una vez guardado se pueden crear las tablas estadísticas según correspondan.

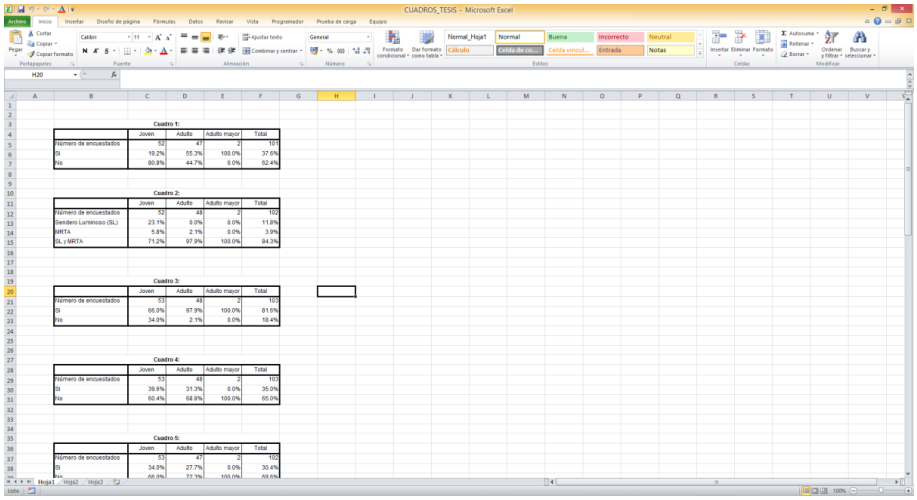




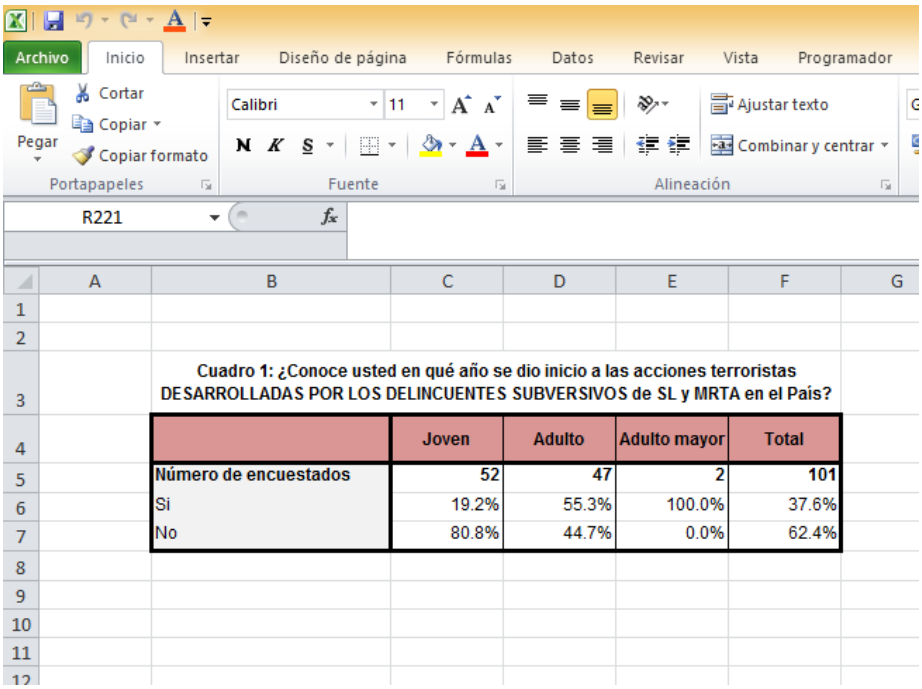
- **Programa N°03: MS EXCEL**

MS EXCEL es un programa que permite manejar bases de datos, crear tablas, gráficos, etc. El proceso que se utilizó para la elaboración de los cuadros estadísticos para el presente trabajo fue el siguiente:

1. Primero debemos de pegar las tablas creadas en el SPSS al Excel de forma normal.



2. Luego se aplican los colores para mejorar la presentación de las tablas. Con el botón marcado



Cuadro 1: ¿Conoce usted en qué año se dio inicio a las acciones terroristas DESARROLLADAS POR LOS DELINCUENTES SUBVERSIVOS de SL y MRTA en el País?

	Joven	Adulto	Adulto mayor	Total
Número de encuestados	**52**	**47**	**2**	**101**
Si	19.2%	55.3%	100.0%	37.6%
No	80.8%	44.7%	0.0%	62.4%

3. Ahora creamos las gráficas. Para este caso utilizaremos dos tipos de gráficas. Primero la gráfica de barras que mostraran los distintos porcentajes por cada estrato de edad. Y las llamadas tortas o pies que mostraran los porcentajes totales.

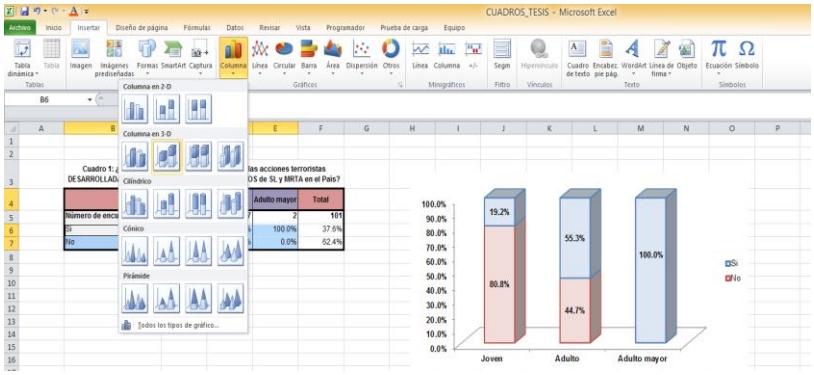
   - <u>Para las barras</u>

     a. Primero marcamos las áreas donde se encuentra la información a mostrar.

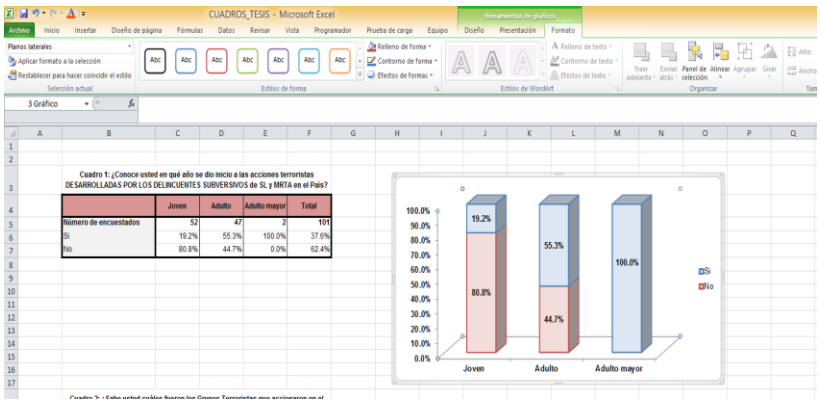
Cuadro 1: ¿Conoce usted en qué año se dio inicio a las acciones terroristas DESARROLLADAS POR LOS DELINCUENTES SUBVERSIVOS de SL y MRTA en el País?

	Joven	Adulto	Adulto mayor	Total
Número de encuestados	52	47	2	101
Si	19.2%	55.3%	100.0%	37.6%
No	80.8%	44.7%	0.0%	62.4%

     b. Creamos los gráficos.



     c. Luego le damos formato a los gráficos para mejorar la presentación.



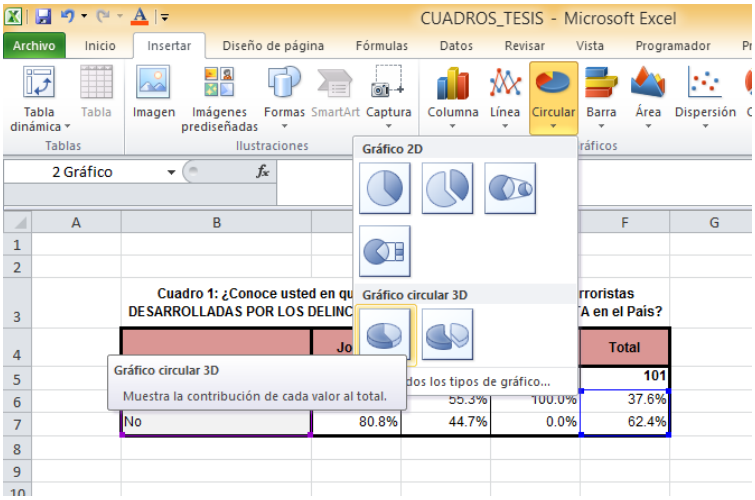
- Para los pies

a. Marcamos el área donde se encuentran los datos a mostrar.

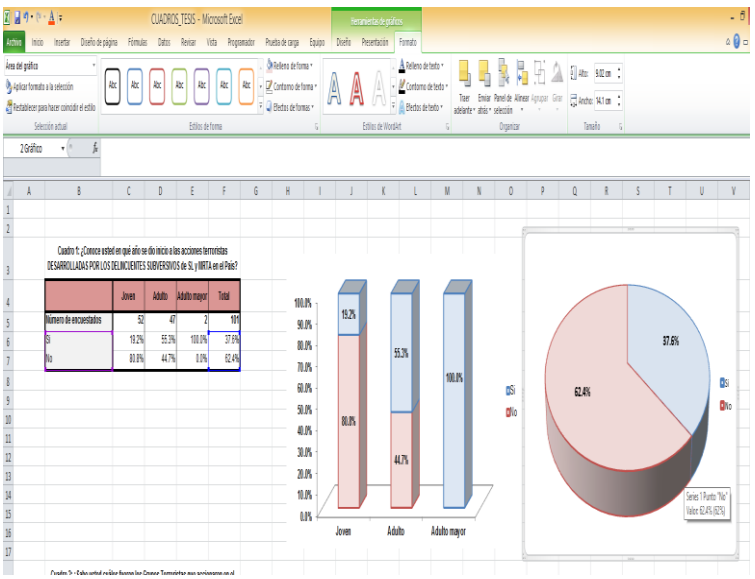
Cuadro 1: ¿Conoce usted en qué año se dio inicio a las acciones terroristas DESARROLLADAS POR LOS DELINCUENTES SUBVERSIVOS de SL y MRTA en el País?

	Joven	Adulto	Adulto mayor	Total
Número de encuestados	52	47	2	101
Si	19.2%	55.3%	100.0%	37.6%
No	80.8%	44.7%	0.0%	62.4%

b. Crearnos la graficas.



c. Damos formato.



7.4. Diseño estadístico

Como ya se ha explicado, las estadísticas fueron diseñadas para conocer cómo la población percibe la amenaza terrorista y ciberterrorista en nuestro país y a nivel global. La información obtenida no altera las hipótesis iniciales ni sus variables, pero comprueba varios puntos mencionados en la presente investigación, como desconocimiento de uno de los sectores, pobre inversión educacional, desconocimiento de la presencia digital, entre otros. Los datos han sido aceptados como son, como datos, pero ellos no fueron el principio de esta tesis y debe entenderse que, de no existir estos datos, las hipótesis presentadas seguirían teniendo el mismo resultado. Esto solo fue elaborado bajo una percepción social y crítica.

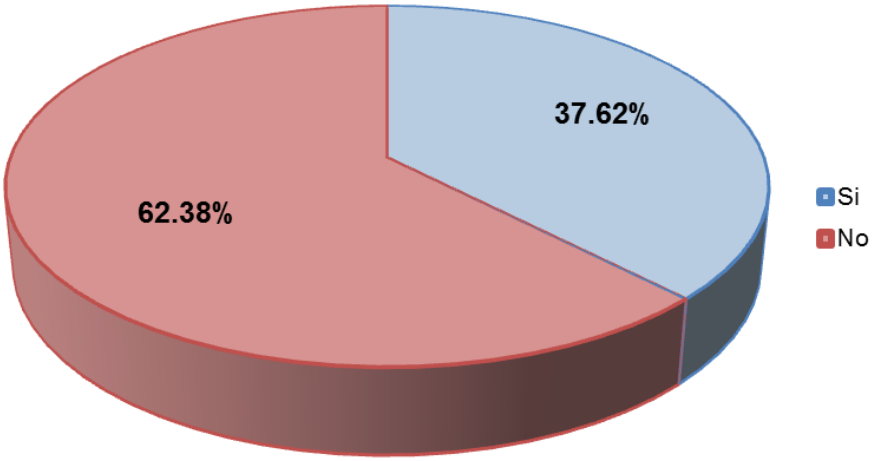
Cada una de las preguntas efectuadas cuenta con tres puntos.

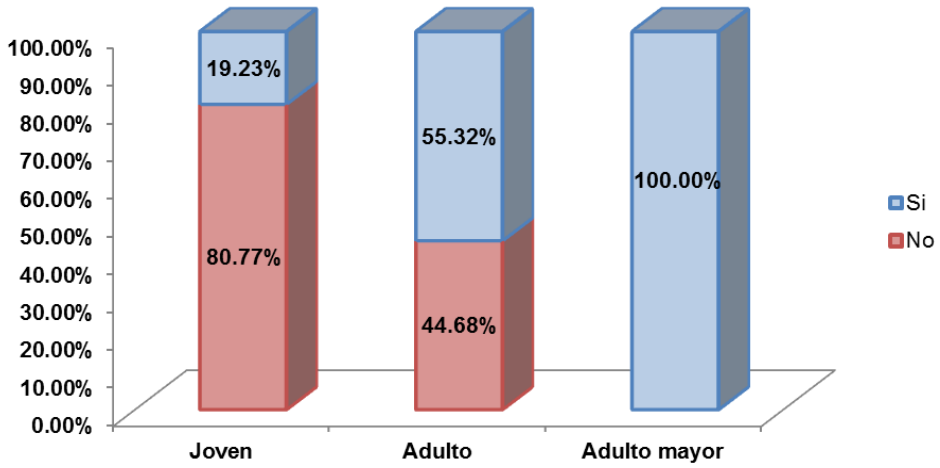
- Punto 1: Pregunta formulada y resultado con número de personas y porcentajes estadísticos.
- Punto 2: Grafico en 2D en forma de dona, con porcentaje señalado como resultado de la pregunta efectuada.
- Punto 3: Gráfico en 2D en forma de barras con porcentaje señalado como resultado de la pregunta efectuada.

Finalmente, el resultado total de las preguntas y gráficas cuenta con una descripción dando mayor descripción a los resultados obtenidos a lo largo del cuestionario y la investigación. Fueron un total de 13 preguntas que ayudaron a comprobar el conocimiento de la población en diversos estratos sociales; pero, es importante recordar, que estas respuestas no son influyentes al resultado final, solo ocupan un marco de conocimiento para el investigador con relación al entendimiento de la población nacional sobre el ciberterrorismo y las amenazas terroristas.

Cuadro 1: ¿Conoce usted en qué año se dio inicio las acciones terroristas desarrolladas por los delincuentes subversivos de SL y MRTA en el país?

	Joven	Adulto	Adulto mayor	Total
Número de encuestados	**52**	**47**	**2**	**101**
Si	19.23%	55.32%	100.00%	37.62%
No	80.77%	44.68%	0.00%	62.38%



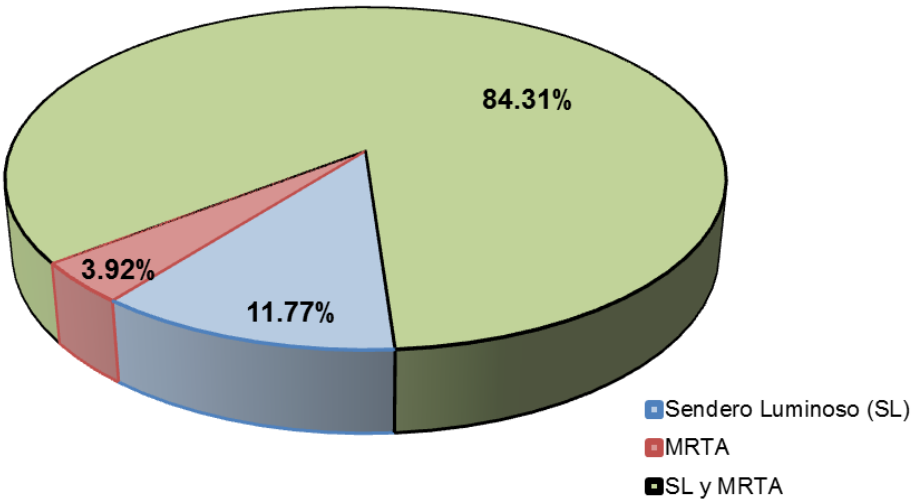


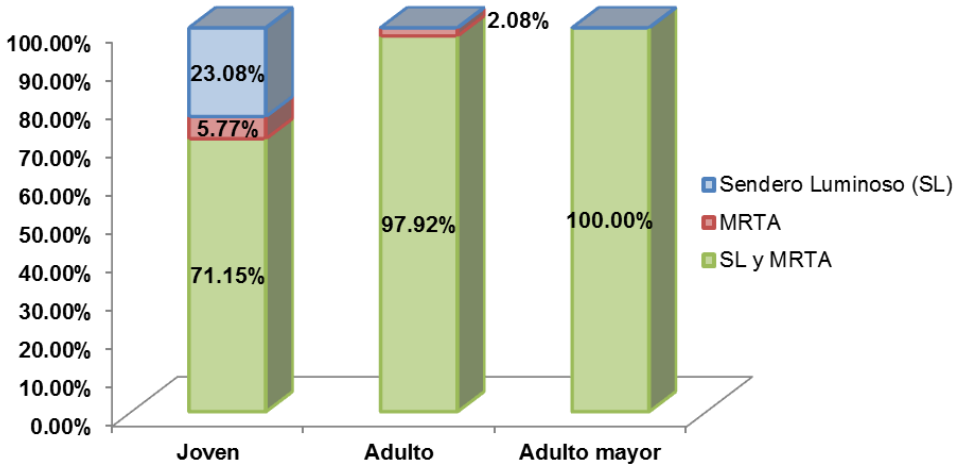
***Descripción*:**

El 80.77% de los jóvenes desconoce el año de inicio del accionar de SL y MRTA, siendo el porcentaje más elevado en comparación al de los adultos con 55.32%, reflejando que aún conservan en sus memorias los vestigios de accionar terroristas. El resultado total señala que 62.38% del total desconoce del accionar terrorista en el país. Se comprueba que el eslabón generacional es el más débil, y lo estragos de la falta de educación histórica cae en los jóvenes.

Cuadro 2: ¿Sabe usted cuáles fueron los grupos terroristas que accionaron en el país entre 1982 y 2000?

	Joven	Adulto	Adulto mayor	Total
Número de encuestados	**52**	**48**	**2**	**102**
Sendero Luminoso (SL)	23.08%	0.00%	0.00%	11.77%
MRTA	5.77%	2.08%	0.00%	3.92%
SL y MRTA	71.15%	97.92%	100.00%	84.31%



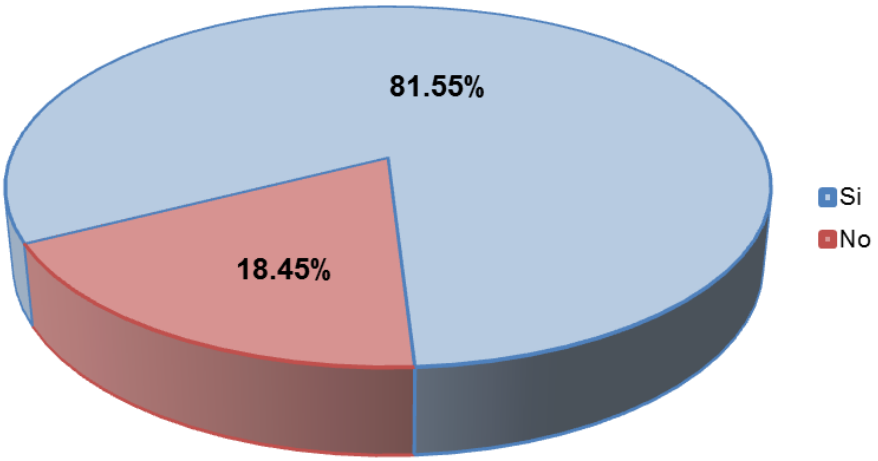


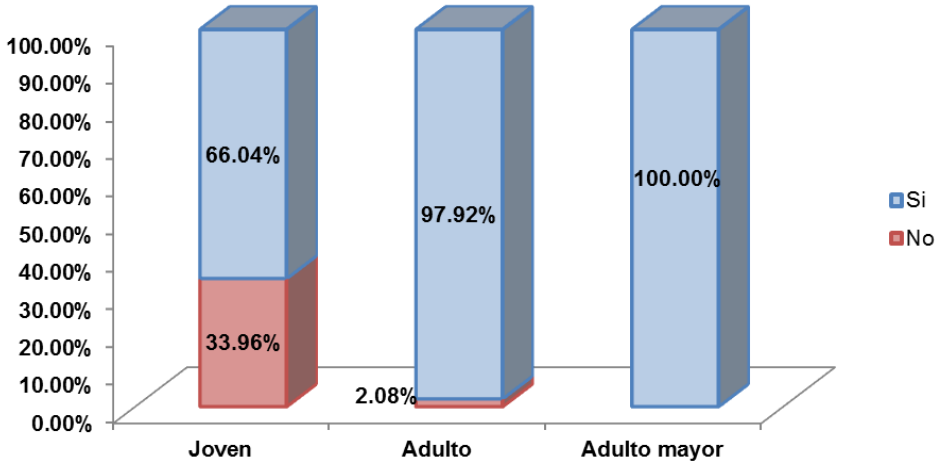
***Descripción*:**

El 84.31% de los encuestados conoce a SL y MRTA. A pesar de no conocer parte de su historia, el 71.15% de jóvenes conoce a ambas organizaciones, el 23.08% solo conoce o ha oído escuchar de SL, y el 5.77% a MRTA. Esto parece debilitar la percepción de desconocimiento de la población formulados en la primera pregunta; no obstante, la información que ellos han recibido ha sido por parte de programas televisivos, Internet o sus padres. El sector educación sigue débil.

Cuadro 3: ¿Tiene conocimiento usted que las acciones terroristas de SL y MRTA provocaron más de 25 mil muertos y la pérdida de más de 25 mil millones de dólares al país?

	Joven	Adulto	Adulto mayor	Total
Número de encuestados	**53**	**48**	**2**	**103**
Si	66.04%	97.92%	100.00%	81.55%
No	33.96%	2.08%	0.00%	18.45%



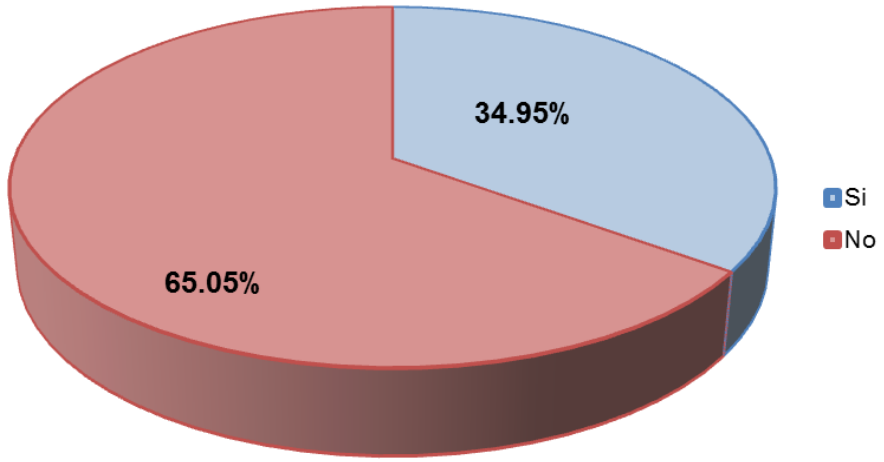


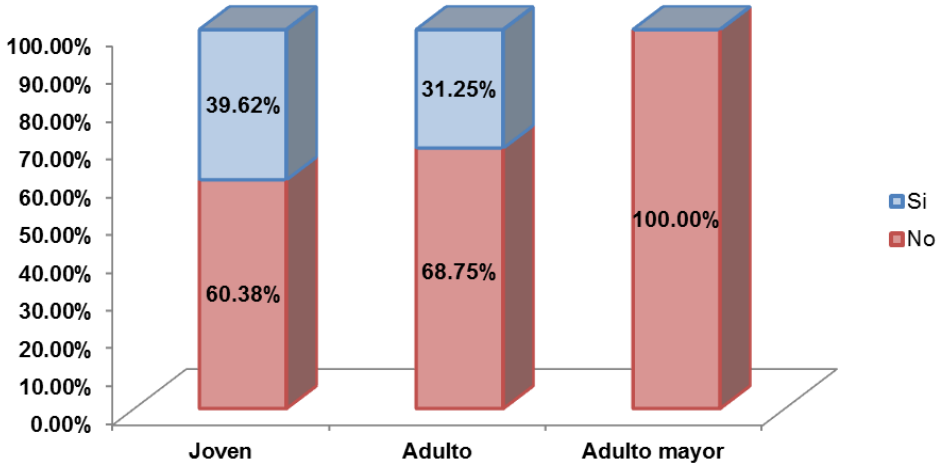
***Descripción*:**

Con un 66.04% son los jóvenes quienes muestran el mayor desconocimiento sobre el saldo de muertos y pérdidas ocasionadas al país durante los años de lucha contra el terrorismo. Una vez más, obtuvieron dicha información por medio de la televisión o Internet, pero ninguno de ellos pudo afirmar que su centro educativo o algún libro educacional que los guiara en épocas escolares les hayan brindado esta información. Por otro lado, los adultos siguen demostrando que la realidad que vivieron es difícil de olvidar. Eso refleja el 97.92% de los encuestados.

Cuadro 4: ¿Cree usted que la captura de los mandos de los grupos subversivos terroristas de Sendero Luminoso (SL) y el MRTA han dado término a la presencia de los grupos terroristas en el país?

	Joven	Adulto	Adulto mayor	Total
Número de encuestados	**53**	**48**	**2**	**103**
Si	39.62%	31.25%	0.00%	34.95%
No	60.38%	68.75%	100.00%	65.05%



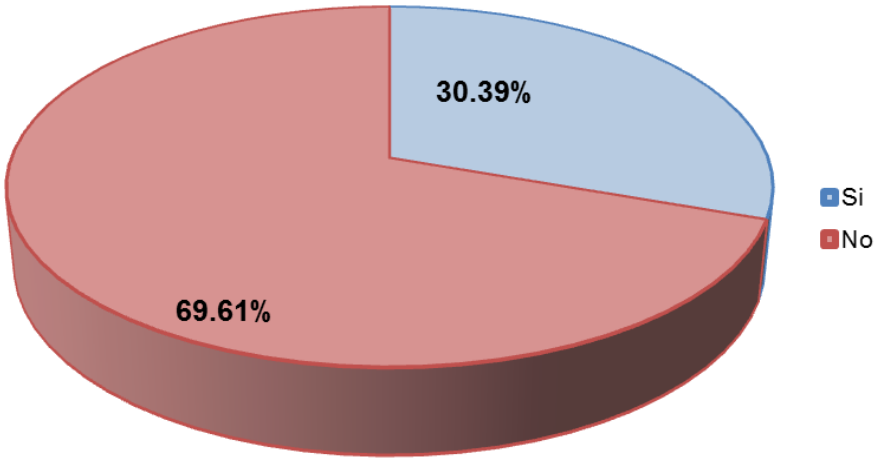


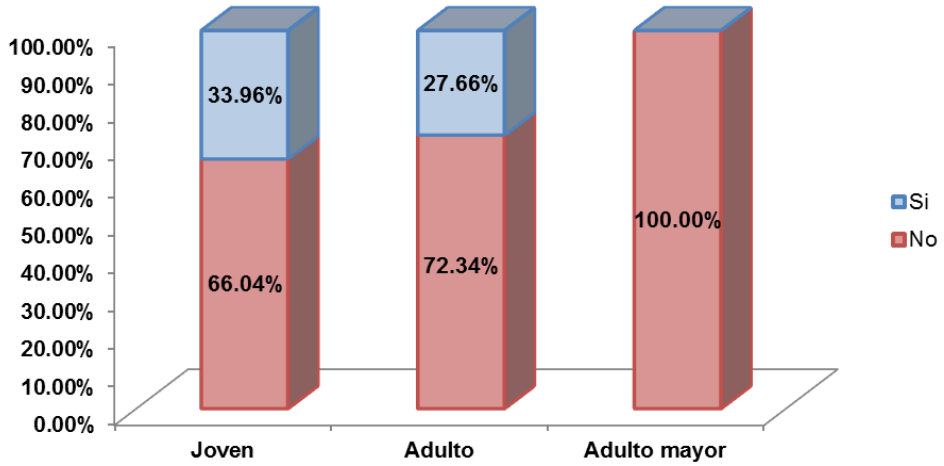
***Descripción*:**

El 65.05% del total de los encuestados creen que aún hay presencia de los grupos terroristas en nuestro país. Tanto jóvenes (con un 60.38%), adultos (con un 68.75%), y adultos mayores (con un 100%) concuerdan con esa respuesta. Solo un 34.95% que considera que las huestes terroristas están extintas en nuestro país.

Cuadro 5: ¿Cree usted que los jóvenes, en nuestro país, conocen verdaderamente del accionar terrorista que vivió el Perú y que causó los daños antes mencionados?

	Joven	Adulto	Adulto mayor	Total
Número de encuestados	**53**	**47**	**2**	**102**
Si	33.96%	27.66%	0.00%	30.39%
No	66.04%	72.34%	100.00%	69.61%



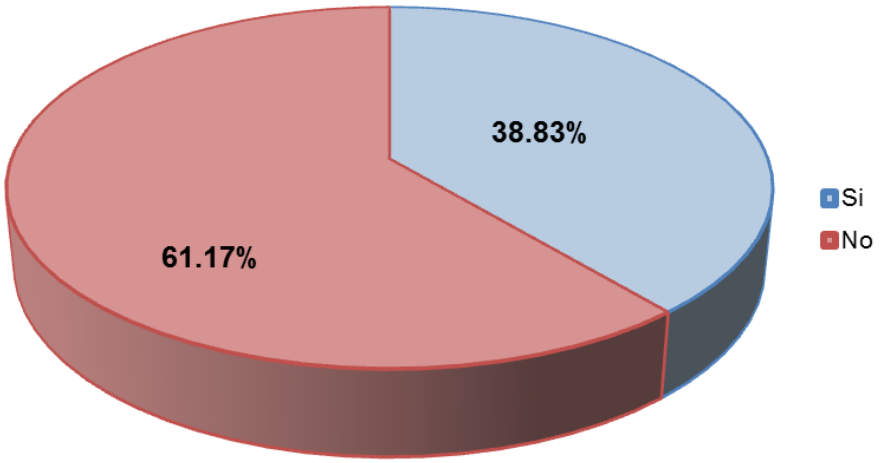


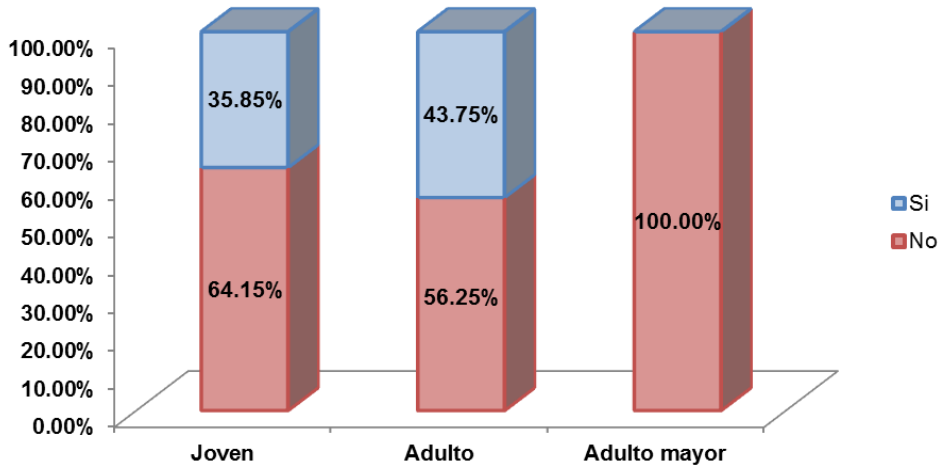
***Descripción*:**

El 69.61% de los encuestados considera que los jóvenes desconocen el accionar del terrorismo que vivió el Perú; y en una especie de *mea culpa*, un 66.04% de la población joven admite el desconocimiento de todo el accionar terrorista, a pesar de haber dicho anteriormente conocer el saldo de muerto y el dinero perdido. Esto demuestra que la juventud es el talón de Aquiles de nuestra sociedad y el sector preferido por los terroristas para su renacimiento.

Cuadro 6: ¿Conoce usted las formas que utilizan actualmente los grupos terroristas para hacer conocer su ideología?

	Joven	Adulto	Adulto mayor	Total
Número de encuestados	**53**	**48**	**2**	**103**
Si	35.85%	43.75%	0.00%	38.83%
No	64.15%	56.25%	100.00%	61.17%



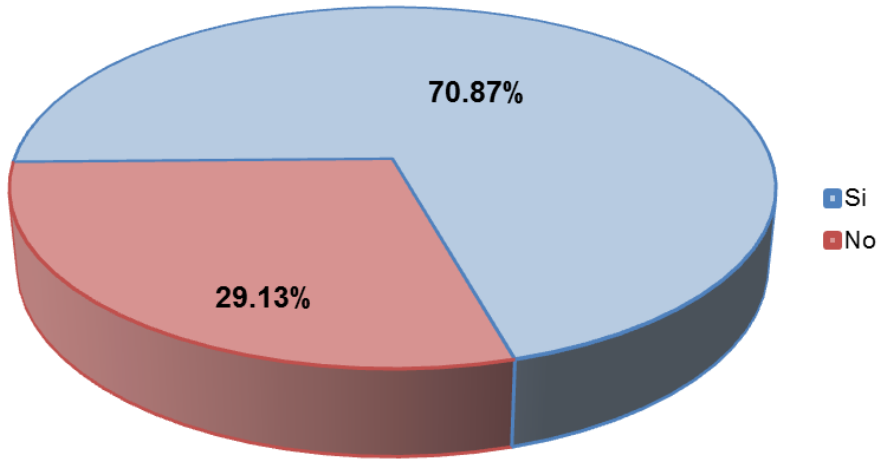


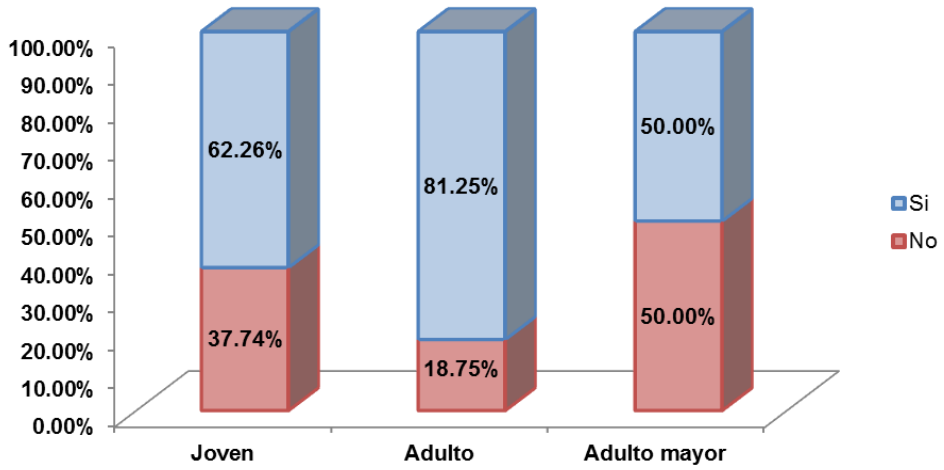
***Descripción*:**

El 64.15% de jóvenes reafirmar su posición de no conocer las metodologías actuales de operación del terrorismo; y el 35.85% que afirma conocer solo sabe de las pintas y la presencia universitaria que ha reingresado con fuerza, pero ese es un método tradicional traído a la actualidad. Tanto el 56.25% de adultos como el 100% de adultos mayores desconocen las nuevas modalidades.

Cuadro 7: ¿Conoce usted que estos grupos terroristas vienen empleando Internet para expandir su ideología?

	Joven	Adulto	Adulto mayor	Total
Número de encuestados	**53**	**48**	**2**	**103**
Si	62.26%	81.25%	50.00%	70.87%
No	37.74%	18.75%	50.00%	29.13%



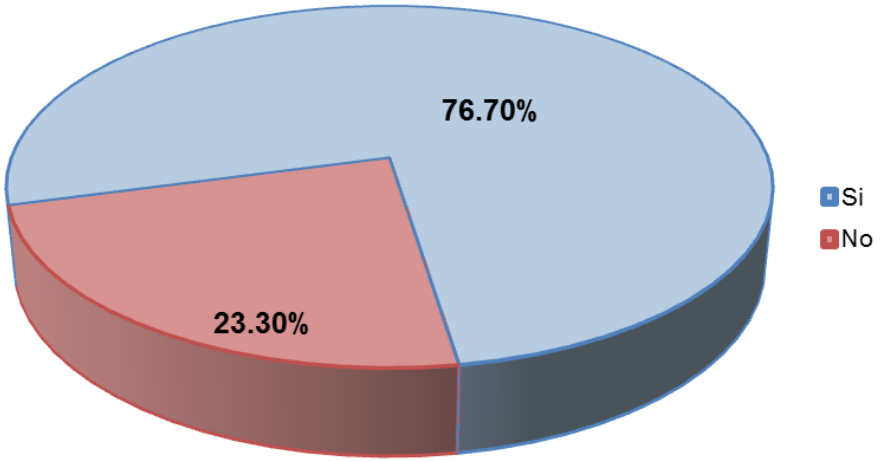


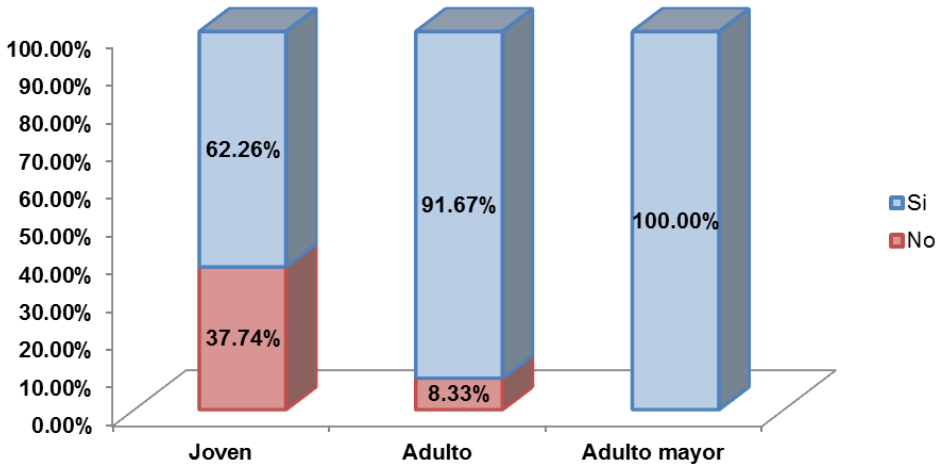
***Descripción*:**

El 70.87% del total de los encuestados conoce que los grupos terroristas vienen empleando Internet para expandir su ideología, tanto en páginas web como en redes sociales. Sectorizando, el 37.74% de jóvenes desconoce de la presencia digital del terrorismo; contraste de alto impacto con el 81.25% de adultos están informados de este hecho.

Cuadro 8: ¿Conoce usted que en el Perú se ha promulgado una Ley de ciberdelitos y una modificatoria?

	Joven	Adulto	Adulto mayor	Total
Número de encuestados	**53**	**48**	**2**	**103**
Si	62.26%	91.67%	100.00%	76.70%
No	37.74%	8.33%	0.00%	23.30%



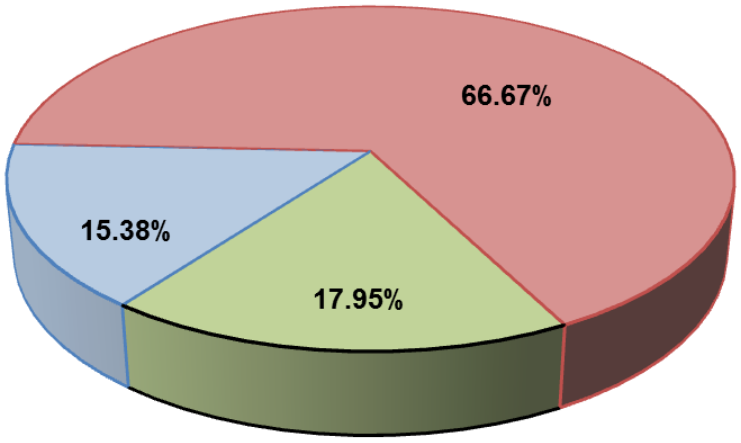


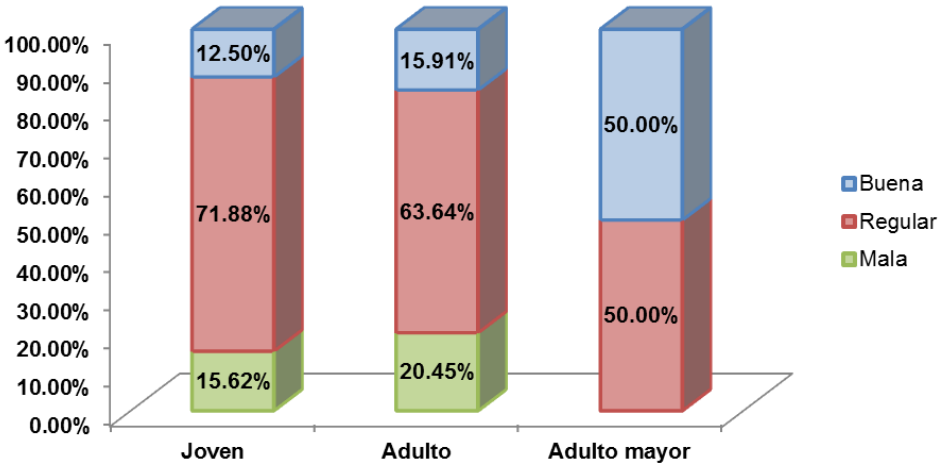
***Descripción*:**

El 23.30% del total de encuestados desconoce la promulgación de la Ley de ciberdelitos y su modificatoria. Sorprende saber que el 76.70% del total encuestado sí conoce sobre ambas normas, lo que a su vez contrasta con lo que dijera la OEA en su informe de seguridad LATAM, que es nuestra falta de conocimiento en normas de índole digital; pero recordemos que son muchas las normas y aquí preguntamos sobre una en específico. Ha pasado tiempo desde su promulgación, por lo que es de mayor conocimiento.

Cuadro 9: Concepto que tiene de la Ley de ciberdelitos y su modificatoria

	Joven	Adulto	Adulto mayor	Total
Número de encuestados	**32**	**44**	**2**	**78**
Buena	12.50%	15.91%	50.00%	15.38%
Regular	71.88%	63.64%	50.00%	66.67%
Mala	15.62%	20.45%	0.00%	17.95%



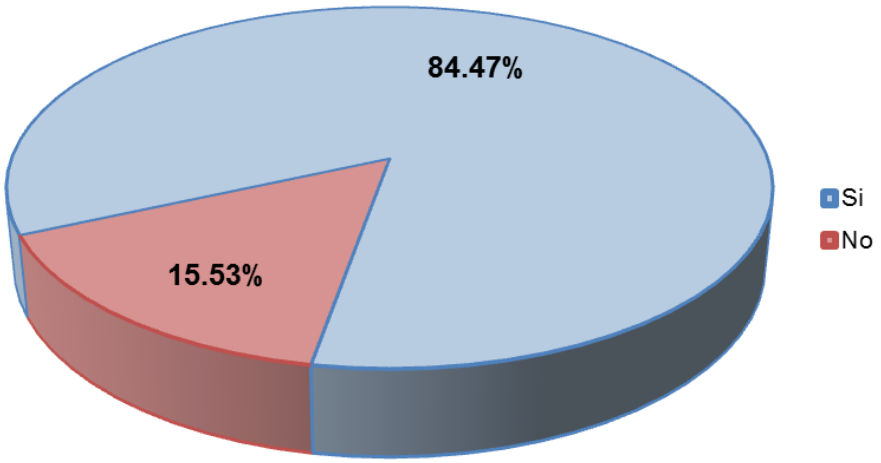


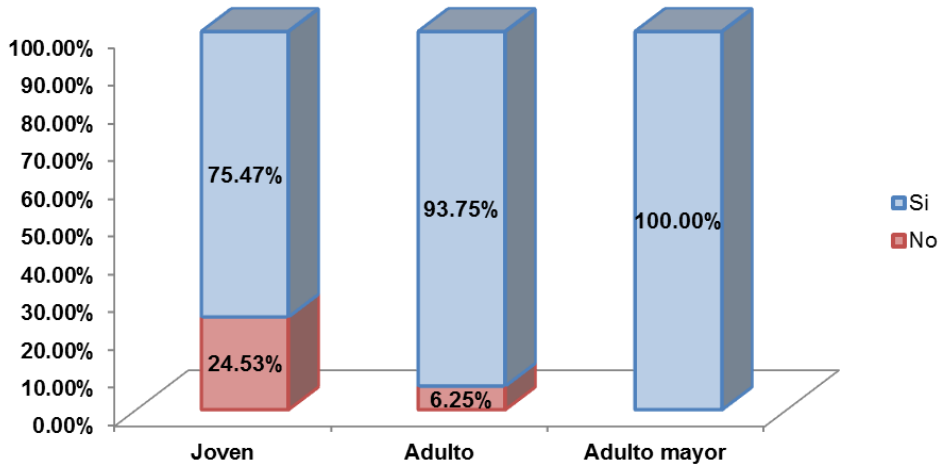
***Descripción*:**

Con relación a la opinión sobre la Ley de ciberdelitos y su modificatoria, un 66.67% del total las consideran regulares; un 15.38% las consideran buenas; y un 17.95% que son malas. Cuando se preguntó por qué las consideraban regulares o malas, afirmaron que sentían que **«no los protegían del todo»**, una respuesta reflejo de un mal trabajo político y en la que debieron enfocarse al momento de elaborar ambas normas que no solo son débiles e ineficientes, sino que dan ventaja al hampa con bastos vacíos legales.

Cuadro 10: ¿Cree usted que existe el ciberterrorismo?

	Joven	Adulto	Adulto mayor	Total
Número de encuestados	**53**	**48**	**2**	**103**
Si	75.47%	93.75%	100.00%	84.47%
No	24.53%	6.25%	0.00%	15.53%



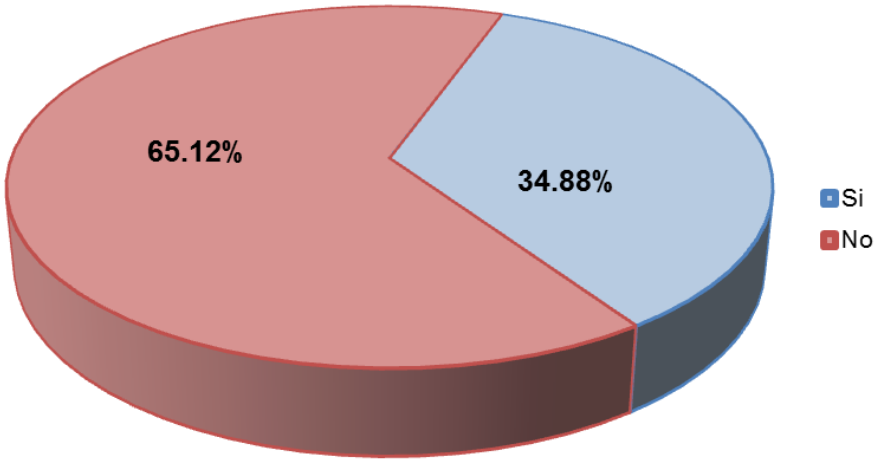


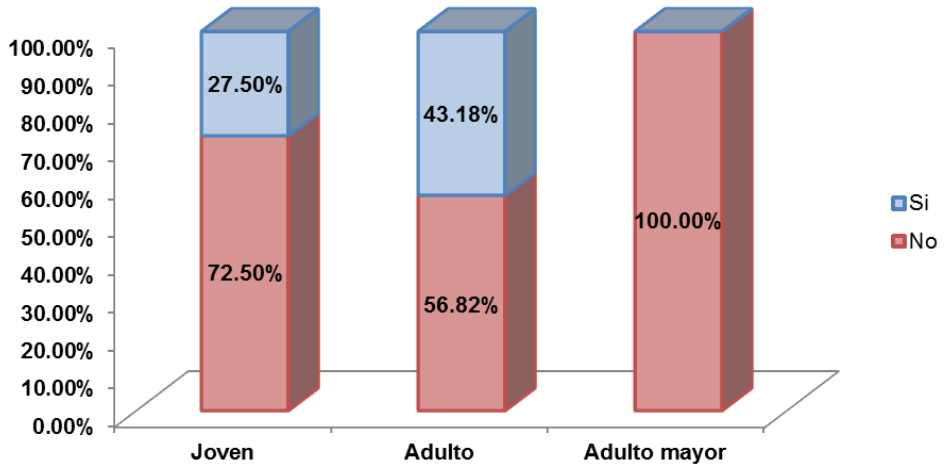
***Descripción*:**

Son muchos los factores que mostraron al ciberterrorismo a la sociedad. Producciones de Hollywood, videojuegos, noticieros, contenido digital, entre otros. Así lo deja ver el 84.47% del total de las personas encuestadas quienes ya aceptan al ciberterrorismo como una realidad —por más que no tengan datos que ayuden a su respuesta—. Solo el 15.53% del total encuestado considera que es una cuestión de fantasía y nada real. Se comprueba que, por más diversas que sean las maneras de llevar el mensaje, la sociedad está consciente de su existencia y como peligro latente.

Cuadro 11: ¿Sabía usted que el ciberterrorismo está considerado como la figura de mayor peligrosidad a nivel mundial?

	Joven	Adulto	Adulto mayor	Total
Número de encuestados	**40**	**44**	**2**	**86**
Si	27.50%	43.18%	0.00%	34.88%
No	72.50%	56.82%	100.00%	65.12%



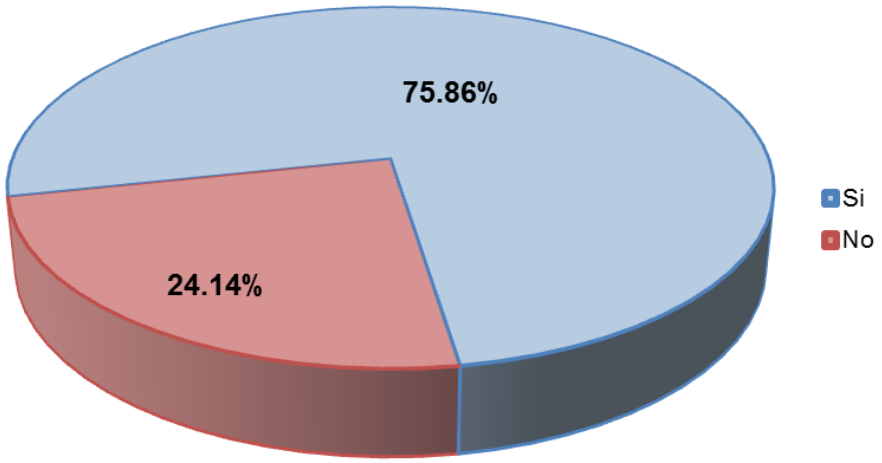


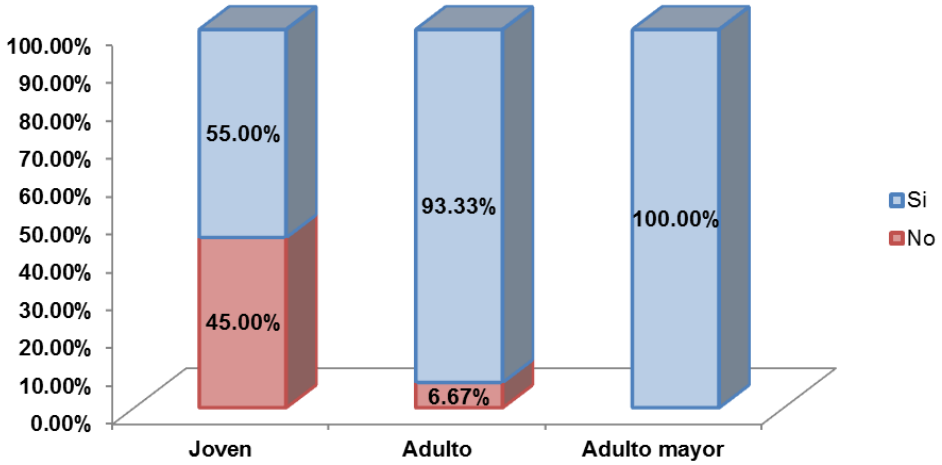
***Descripción*:**

Regresando a lo explicado en el anterior cuadro, si bien se había afirmado conocer la existencia del ciberterrorismo, un 65.12% del total encuestado niega tener conocimiento que esta figura sea una amenaza global y de alta peligrosidad. Si bien la población joven navega más en Internet, del 75.47% que creen que existe el ciberterrorismo (cuadro 10), el 72.50% lo desconoce cómo la figura de mayor peligrosidad en el mundo; De igual forma con la población adulta, donde el 93.75% afirmaba conocer esta figura (cuadro 10), un 56.82% también afirman desconocer su grado de importancia y peligrosidad a nivel mundial.

Cuadro 12: ¿Sabía usted que el ciberterrorismo no solo se refiere a acciones realizadas por grupos subversivos?

	Joven	Adulto	Adulto mayor	Total
Número de encuestados	**40**	**45**	**2**	**87**
Si	55.00%	93.33%	100.00%	75.86%
No	45.00%	6.67%	0.00%	24.14%



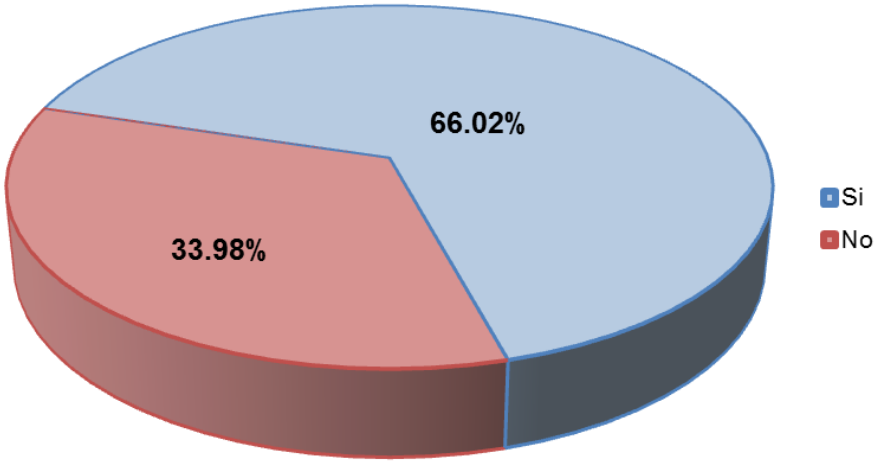


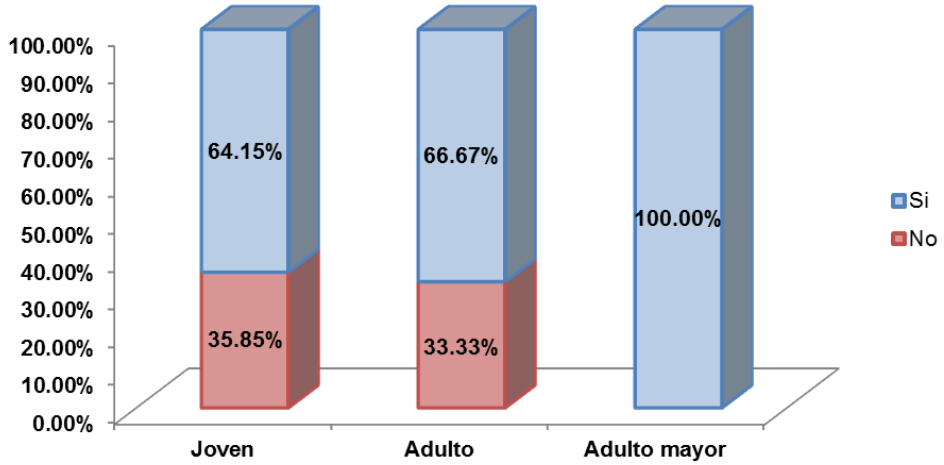
***Descripción*:**

Del 75.47% de los jóvenes que aceptan la existencia del ciberterrorismo (cuadro 10). el 45% desconoce que el ciberterrorismo no solo se refiere a acciones realizadas por grupos subversivos; al igual que del 93.75% de adultos encuestado (cuadro 10), el 6.67% lo desconoce. Por último, el 75.86% del total encuestado, a pesar de lo dicho anteriormente, está seguro de que al hablar de ciberterrorismo hace referencia a todas las vertientes terroristas y no solo subversivo terroristas. El sector adulto y adulto mayor son más conscientes de la figura que pueda tener el ciberterrorismo, a pesar de no tener más datos de los recibidos en noticias y otros medios.

Cuadro 13: ¿Piensa que el terrorismo sigue vigente en el país?

	Joven	Adulto	Adulto mayor	Total
Número de encuestados	**53**	**48**	**2**	**103**
Si	64.15%	66.67%	100.00%	66.02%
No	35.85%	33.33%	0.00%	33.98%





***Descripción*:**

Del total de encuestados, el 66.02% piensa que el terrorismo aún sigue vigente en el país, no solo por su presencia aún latente en el VRAEM, además por los reportes periodísticos difundidos en todos los medios de comunicación, y las amenazas que se pueden ver día a día por los mismos medios; más aún, por el grupo de terroristas liberados en el transcurso de los años por ineficiencia política u otros intereses. Esto ha permitido darnos cuenta de que, a pesar de los años, este es un mal aún latente en la memoria de los peruanos y en el que no se ha trabajado mucho políticamente hablando. El problema será mayor cuando el ciberterrorismo tome ventaja.

CAPÍTULO IV
PRESENTACIÓN – RESULTADO

1. Contrastación de hipótesis

La base de la hipótesis buscaba demostrar que la figura del ciberterrorismo no solo consistía un peligro para nuestro país; sino también, que debía ser considerada como una figura delictiva dentro de nuestra legislación. A raíz del desarrollo de esta investigación se ha presentado un sinfín de pruebas extraídas de medios periodísticos que comprueban la peligrosidad y crecimiento de una figura como esta. Por otro lado, las encuestas han demostrado que el país no está preparado para una amenaza como esto, ignorando incluso su existencia.

Asimismo, el que SL ya tenga presencia en redes y en las actividades de los jóvenes constituye un peligro a largo plazo que nuestros legisladores no han percibido, y eso si lo vemos desde la capa superficial de Internet. No se tienen datos de las dos capas restantes que son la Deep web y la Dark web, pero no se descarta presencia o principios de presencia como otros grupos ya lo tienen.

Finalmente, los informes presentados por las diversas organizaciones internacionales y las opiniones de los principales expertos en diversos sectores dejan en claro que el ciberterrorismo sí es una amenaza real y que es responsabilidad de cada país prepararse para enfrentar a esta epidemia que se expande por el ciberespacio y que tienen como único propósito la destrucción.

2. Análisis e interpretación

Cada uno de los **datos presentados en esta investigación** como las entrevistas, los informes y las notas provenientes de los *journals* especializados ha sido cuidadosamente analizado y comprobados como fuente antes de ser utilizarlo para dar sustento a las explicaciones que se manejaban con cada uno de los temas expuestos. Se recolectó información por más de cinco años, por lo que se manejó los contenidos más actuales y existentes hasta el momento. Uno de los mayores inconvenientes es que no existe bibliografía jurídica en la materia más que la Tesis presentada por el autor en el año 2014, que tiene muchas variables para la investigación actual, pero que sirvió de base para el desarrollo de muchos puntos.

En cuanto a la **población encuestada**, su información personal se mantuvo en estricta privacidad, respetando la normativa existente en materia de protección de datos personales (Ley N°29733 y Reg. DS. N°003-2013-JUS; Mod. DL N°1353), por lo que solo se dio a conocer sus respuestas. Los encuestados pertenecen a diversos sectores socioculturales del país y fueron encuestados en diversos días, en ambientes sin ruido y sin presión para que las respuestas que dieran en el cuestionario entregado fueran las más sensatas e imparciales posibles.

Por último, toda la **información obtenida** permitió comprobar la hipótesis, demostrando que el ciberterrorismo si es una amenaza real en el mundo actual y que el Perú no se encuentra preparado, ni jurídicamente, ni con mecanismos de defensa

cibernética, ni mucho menos con una población preparada y conocedora de la amenaza. Todavía hay una latente que es la investigación realizada por parte del Estado, de la cual no hay existencia, por lo que aún no se tienen cifras de cuanta acción tienen los grupos terroristas nacionales en el país; no obstante, su presencia está marcada por redes sociales y páginas web, por lo que, de aquí en adelante, será trabajo del Estado peruano presentar las cifras, que solo comprobaran que el ciberterrorismo es una amenaza real, como ya quedó explicado en cada una de las páginas de esta investigación, que deja la puerta abierta para futuros trabajos que quieran centrarse en esta materia o en el campo de los ciberdelitos y la ciberdelincuencia.

CAPÍTULO V
DISCUSIÓN

1. Discusión

Quizás el mayor problema que se encontró durante el desarrollo de esta investigación fue la búsqueda de material bibliográfico jurídico en materia de ciberterrorismo. No existe, por el momento, una opinión escrita o investigación resaltante que siga los cánones del mundo de las leyes y la doctrina jurídica; pero, eso no fue impedimento para continuar con esta tesis. Este tropiezo pudo ser compensado rápidamente con la rica literatura albergada en *journals* especializados, informes realizados por instituciones importantes y respetables, investigaciones publicadas en diarios y reportajes, todos ahora de fácil acceso gracias las ventajas de Internet.

Las entrevistas que brindaran los especialistas colocaron cimientos más fuertes a la hipótesis presentada. Sus experiencias reflejadas en sus respectivos campos brindaron una única respuesta, y es que el ciberterrorismo es una amenaza real, constante y en crecimiento, por lo que es responsabilidad de cada país ir preparándose para hacer frente a las amenazas que este genera.

En visión nacional, no estamos a la par de muchos países que ya cuentan con equipos de respuesta ante amenazas o que tienen una idea de cómo hacer frente a la ciberdelincuencia desde un sector legal. Tenemos mucho camino por recorrer y esto se ha visto contrastado con cada punto desarrollado y que nos deja la interrogante de saber si realmente tenemos las intenciones de querer luchas contra esta amenaza o esperar primero sus resultados para tomar cartas en el asunto. Sea cual fuere el caso, tenemos muchos años de atraso, lo que seguirán aumentando con el paso de las horas y la tecnología

2. Conclusiones

Quedando comprobada la hipótesis inicial, y luego de un trabajo de más de cinco años de investigación, decir que solo se concluye que el ciberterrorismo es una amenaza existente es no darles importancia a los otros puntos que también se debelaron en el transcurso del tiempo.

1º. La sociedad actual en el Perú ha olvidado la historia de la lucha contra el terrorismo y la subversión; esto se ha visto mayormente reflejado en el impacto que generan movimiento como FUDEPP y MOVADEF en los jóvenes, ahora abanderados de una lucha que no incluye armas, pero sí la misma ideología. Esto constituye una amenaza cuya metodología tendría mayor impacto con el uso de Internet y las TIC.
2º. El desconocimiento de la historia causa otra desventaja, y es que, al parecer, existe una despreocupación por parte del sector educativo de enseñar los sucesos que marcaron parte de nuestra historia republicana, impidiendo que con ello podamos evitar los errores del pasado. Esto se ha visto reflejado en la población joven, que en su mayoría no puede detectar a las figuras principales del terrorismo y mucho menos hablar de ello.

3º. En cuanto a la ley de ciberdelitos actual en el Perú, existen opiniones divididas. Algunos juristas consideran que es un buen avance para nuestro país; pero el sector *hacking* lo considera mala por sus bajísimas penalidades y falta de relación con la realidad. Es esta visión la que se comparte durante toda la investigación; y más aún, porque son muchas instituciones internacionales que opinan lo mismo, por lo que es preciso decir que no contamos con una ley adecuada para combatir la ciberdelincuencia y, mucho menos, el ciberterrorismo.
4º. Cierto sector de la juventud ya ha caído en la ideología terrorista --como se ha podido comprobar durante el desarrollo de la investigación--, la que buscan justificar por el mismo desconocimiento que se tiene de los sucesos que se dieron desde la década de los 80s.
5º. La población, en su mayoría, desconoce cómo operan actualmente los grupos terroristas para sus diversas finalidades —como el empleo de web y redes sociales—, y si es que los grupos terroristas y subversivas tradicionales que actualmente luchan por renacer utilizan estos métodos para captar jóvenes o expandir su ideología. Esto hace más difícil el trabajo de denunciar dicho contenido alojado en la red.
6º. La encuesta–estudio de campo realizado demostró que las personas de edad adulta, entre los 30 a 59 años, tienen conocimiento de la amenaza que representa el terrorismo y su accionar, sea porque algunos fueron víctimas de dichos actos o por los acontecimientos vividos.
7º. La actual ley de ciberdelitos no es conocida por la mayoría de la población, y muchos menos se tiene conocimiento si es que el ciberterrorismo ha sido considerado para formar parte de los delitos que la norma tiene en su haber; mucho menos saben que esta figura ha sido considerada la más peligrosa a nivel internacional.
8º. El alcance la tecnología ha superado las expectativas de años anteriores, construyendo en nosotros una especie dependiente de la misma. En el caso del ciberterrorismo, esto se refleja como una ventaja para su accionar. Recordemos los ejemplos presentados en la investigación que parten desde la apología en redes hasta las comunicaciones encriptadas en sistemas de videojuegos.
9º. Los movimientos terroristas han aprendido a como captar a la juventud para unirse a su bando. Para ello emplean estrategias ciberterroristas y psicología para manipular a este sector. Recordemos las versiones alternativas de títulos importantes de videojuegos que han tenido un gran número de descargas y que han servido para expandir su visión del mundo y su deseo de nuevos reclutas para su guerra.
10º. Se ve necesario la preparación de un equipo de respuesta especializado para combatir el ciberterrorismo, con la tecnología precisa para estar a la par de la amenaza. Esto constituye una gran inversión por parte del Estado y de alianza con los países más avanzados en estrategia y lucha contra la ciberdelincuencia.

3. Recomendaciones

Con la hipótesis principal y las hipótesis secundarias comprobadas, es necesario brindar algunas recomendaciones que, a largo plazo, pueden ayudar a combatir una amenaza como el ciberterrorismo; y, a corto plazo, darnos los parámetros suficientes para luchar contra la ciberdelincuencia.

1º. Se debe redireccionar el sector académico y hacer una inversión en capital económico y humano en áreas de investigación centradas en el derecho, la tecnología y la ciberseguridad. Este es un punto fundamental que ha permitido a muchos países trabajar mejor en sus proyectos legislativos, ya que cuenta con un respaldo de un sector muchas veces rezagado, pero consiente de los constantes cambios que se producen en la materia. La investigación es la primera clave para nuestro avance.
2º. Se hace necesario una modificatoria a la malla curricular para ingresar una actualización al derecho y establecer la materia de ciberderecho y gobernanza de Internet como obligatorias. Esto permitirá forjar abogados preparados y consientes de los cambios del mundo para hacer frente a los ciberdelitos, así como tener una futura cartera de jueces y fiscales capacitados desde la cantera universitaria para sus respectivas funciones durante un proceso que implique materias tecnológicas y terminología avanzada.
3º. Es indispensable el ingreso de una nueva materia universitaria y técnica centrada en la ciberseguridad y temas afines, para así contar con profesionales que hagan frente a las adversidades que atraviesa y atravesará el país en el transcurso de los años. Además, este tipo de profesionales aumentará su demanda, y que mejor que ya contar con un equipo de trabajo educado desde las aulas.
4º. Trabajar en una modificación de la actual ley de ciberdelitos para que esta tenga un contenido más acorde con la realidad y bajo los estándares internacionales que establecen diversas organizaciones. Así mismo, esto permitirá que el país ingrese a la lista de los países miembros del Convenio de Budapest, lo que traería una gran ventaja en la lucha contra la cibercriminalidad.
5º. Una vez reconocido como delito la figura del ciberterrorismo, trabajar en una ley especial que nos brinde las armas jurídicas para hacer frente a esta amenaza.
6º. Trabajar en un programa de educación dirigido a escolares y universitarios a fin de enseñar los hechos que marcaron la época de la lucha contra el terrorismo, así como hacerlos conocedores de las normas que los protegen tanto en el campo físico como virtual.
7º. Una vez comprendido que la ciberseguridad también forma parte de la seguridad ciudadana, generar programas que estén direccionados a la educación y protección de la población en el campo digital. Es recomendable establecer alianzas con centros educativos, así como con comunidades para dar capacitaciones y expandir la finalidad del programa de manera más rápida y efectiva.
8º. Se hace necesaria la creación de un nuevo equipo de trabajo en el campo de la ciberseguridad; y, siguiendo el ejemplo de los países más fuertes en este campo, darles formación teórica y técnica constante, preparándolos no solo para la amenaza que representa la figura del ciberterrorismo; sino, también, para una posible ciberguerra.

4. Aportes del investigador

4.1. El triángulo de trabajo colaborativo: Estado, ingenieros en ciberseguridad (*hackers*) y abogados para la gestación de una correcta ley en ciberterrorismo y un futuro equipo de respuesta ante el cibercrimen

La creación de la primera y la segunda norma centrada en ciberdelitos en el Perú, así como proyectos y normas adjuntas generadas en el transcurso de los años,

siempre han tenido el mismo error, y es que no se considera al sector técnico o *hackers* para las discusiones que se establecen en las mesas de trabajo. El principal problema es que el excesivo protagonismo del sector jurídica ha causado un constante perjuicio en materia de Internet y seguridad en el campo digital; y es que este sector no conoce cómo funciona el ambiente, solo conoce de leyes y —muchas veces— trabaja con normas desactualizadas.

En el *OAS-First Cyber Security Symposium* (Colombia, 2016) se presentó el primer aporte de esta tesis llamada el **«Triángulo colaborativo»** que resalta la presencia de *hackers*, abogados y Estado y los invitaba a dialogar y trabajar en una misma mesa. Si bien el concepto fue muy bien recibido por los sectores asistentes —academia, sociedad civil y fuerza armada—, es importante decir que este triángulo ya establece personajes y funciones que sí o sí deben respetarse y no modificarse para hablar de un plan exitoso.

Es así como el sector de la seguridad cibernética, representada por los *hackers*, darían los puntos base de los principales problemas que habitan en la red, cuál es el porcentaje de ello, como actúan los ciberdelincuentes y cómo funciona realmente el empleo de la tecnología. Ellos son los que mejor conocen como se desarrolla esa cibercomunidad y saben de sus principales problemas.

Una vez comprendido esto, el sector jurídico tiene la responsabilidad de presentar el primer bosquejo de normas que no violenten los derechos en Internet y que sean un reflejo de lo dicho por los primeros participantes, para ser nuevamente debatida por los presentes llamados a las diversas mesas de trabajo que se creen. La finalidad es generar una norma lo más acorde a la realidad, pero tampoco limitativa por el paso del tiempo. Debe ser una norma que, al igual que Internet, se adapte al cambio constante.
En primera instancia —y debido a las experiencias conocidas y expuestas en este trabajo—, el sector Estado tenía una presencia más limitada centrada a aporte económico y respuestas inmediatas antes las propuestas dadas. Sin embargo, el Estado tiene muchos cuerpos que no se pueden dejar de lado. Es así como la experiencia de las fuerzas armadas será fundamental para también tener una ley que los defienda jurídicamente ante cualquier problema que pueda suscitarse; del poder judicial, conocer sus principales debilidades y dar paso al entendimiento por su parte de cómo funcionará esta norma. El Congreso y los restantes deberán estar presentes para la aprobación de la norma y aporte económico necesario.

No podemos descartar al sector académico y sociedad civil, ubicando al primero en los dos primeros grupos mencionados; y al segundo, como defensa de los ciudadanos y sus derechos, en el sector Estado.

Esta es una manera simple de representar al **«Triángulo colaborativo»**, que ya tienen dos sectores dispuestos a trabajar, que son el Estado —en donde también está la sociedad civil— y los *hackers* —en donde también está la academia—. El talón de Aquiles sigue siendo el sector jurídico; que, a pesar de los años, sigue engañado creyendo que *hacker* es un sinónimo de delincuente, y están obstinados a no sentarse a trabajar con ellos, tanto la generación que ya está por irse, como aquellos de la nueva guardia educados bajo los estigmas del pasado. Será necesario encontrar un nuevo grupo de juristas que esté dispuesto a trabajar en

este triángulo. Esa es la tarea más difícil, pero no imposible. De lograrlo, tal cual se explicó en el *OAS-First*, daríamos el primer paso importante en nuestra historia republicana en la lucha contra los ciberdelitos y el ciberterrorismo.

4.2. Propuestas para la aceptación de la figura del ciberterrorismo como delito dentro de nuestra normativa nacional

Podemos seguir insistiendo que la figura del ciberterrorismo debe ser aceptada por nuestro país como una amenaza, un delito naciente e, incluso, una epidemia o una nueva modalidad empleada por el terrorismo antiguo; sin embargo, son los estudios de organizaciones internacionales, empresas dedicadas a la ciberseguridad y expertos en la materia los que establecen el principal sustento para hablar de una vez por todas sobre la ilegalidad del ciberterrorismo en el Perú.

Las normas que tenemos —de acuerdo con los estudios presentados— no nos protegerán contra las amenazas latentes y crecientes, menos contra la figura del ciberterrorismo. Se sigue pensando que basta con la norma que tenemos para adaptarla a los hechos reales, pero esas normas son temporales, tienen un espacio definido y fueron hechas antes de que el mundo se vinculara con la tecnología e Internet; y si bien estos tienen manejo humano, su conducta no se ve reflejada en los parámetros legislativos actuales, ni siquiera, en la propia ley de ciberdelitos, mal llamada de delitos informáticos.

No somos un país ciberseguro, y ni siquiera hemos debatido sobre ello en el Congreso de la República o en los foros que se arman cada año en el aniversario de la captura de Abimael Guzmán. Somos un país que se ha quedado con la figura del pasado y se rehúsa a avanzar con los demás países de la región; porque es triste ver que todos discuten sobre ciberdelitos, pero nadie entiende de que se tratan.

En la primera tesis elaborada el 2014, se propuesto establecer un proceso de maduración de la ley de ciberdelitos existente en este entonces —todavía no se generaba la modificatoria—, con tal de conocer los aspectos buenos y malos que nos brindaba la norma. Ha casi cuatro años de esa propuesta, debo afirmar que la modificación debe darse de manera inmediata. No ha traído beneficio alguno y, a la larga, sigue siendo una ventaja para la ciberdelincuencia que ya conoce cada uno de los vacíos legales que esta presenta. Por otro lado, esta modificatoria no debe significar el ingreso forzoso de artículos relacionados a la figura del ciberterrorismo. Sigue siendo recomendable ser tratada como una ley especial en donde ámbitos particulares del ejercicio la confirmen. Insisto que, una vez aceptada la figura del ciberterrorismo como delito, este sea tratado bajo el concepto de delito especial, con sus propios parámetros legislativos. Centraremos el conocimiento en una sola figura y no en un artículo que busque concordancia con sus similares, pues esta figura, de acuerdo con lo anteriormente expuesto en este trabajo, merece un trato particular.

Este es el momento de corregir todas las debilidades y desventaja que ha traído consigo las actuales Leyes, siendo este un tiempo de cambios y mejoras.

4.3. Propuesta para la elaboración de un proyecto de Ley especial para la penalización del ciberterrorismo como figura delictiva reconocida en nuestra nación

En un inicio, se pensó en presentar un proyecto de ley que permitiera sentar las bases de la lucha contra del ciberterrorismo. Es durante el desarrollo de este trabajo y las diversas discusiones que resultaron de este en el transcurso del 2016-2017 que se detuvo esta propuesta porque, siendo sinceros, se podría cometer el mismo error que durante años hemos repetido.

Tal como se explica en el punto del **«Triángulo colaborativo»**, es necesaria la presencia de múltiples sectores, a los que debemos de agregar la academia y la sociedad civil. No puede ejercerse un trabajo parcializado y con apellido para buscar los fines más beneficiosos para el país.

Si queremos un punto de partida, la OEA tiene experiencia ayudando a muchos países con sus estrategias de ciberseguridad. CICTE de la OEA puede ayudar al Perú a dar los primeros pasos y establecer las mesas de trabajo correctas en donde prime la experiencia de todos los sectores y la defensa de los intereses nacionales y no particulares, donde el padrinazgo no tenga cabida y se maneje una meta conjunta que es tener la norma base y final para legislar la figura del ciberterrorismo y, por fin, al ser considerado delito, estar preparado para lo que se aproxima.

4.4. Propuesta de sanciones para penalizar la figura de ciberterrorismo ante la creación de una Ley especial

Recalco una vez más. No puede el trabajo recaer en la figura de una sola persona o institución. La propuesta de Ley debe nacer de una mesa de trabajo acompañada de los elementos que conforman el **«Triángulo colaborativo»** para solo así tener éxito. A pesar de ello me veo en la necesidad de proponer ciertas penalidades, que pueden ser aceptadas o no, pero que darían una base a lo que se puede trabajar en el periodo de vida del triángulo.

Finalmente, debo decir que los aportes que se expondrán tienen sustento en la realidad histórica vivida en el país, así como los principales problemas actuales que rodean a la figura del terrorismo y que puede reproducirse en la figura del ciberterrorismo, teniendo una visión social, de seguridad y legal.

4.4.1. *Eliminación de los beneficios penitenciarios*

En un país sumergido por la inseguridad ciudadana, el sistema de beneficios penitenciarios siempre ha sido el principal problema cuando de delitos de habla; principalmente, porque la sociedad percibe en ellos una ventaja absurda para criminales que fácilmente manipulan su propia conducta para con los demás, dando una imagen que les traiga reducción de sus penas. Es así como una pena impuesta de diez años puede ser reducida a cinco o a tres tanto por buena conducta como por confesión

sincera, aplicándose los famosos 2x1 y 3x2, términos usados por los penalistas para dar una explicación más simple a lo expuesto. La pregunta base será si es factible darle beneficios a los ciberterroristas como ya se ha visto con algunos delitos, incluso con el de terrorismo.

Recordemos que, en la década de los 90s, se promulgaron diversos instrumentos legales que impedían a un sentenciado por terrorismo sostener al beneficio penitenciario[122], lo cual cambió con la Sentencia del Tribunal Constitucional Exp. N°010-2002- AI/TC (03 de enero de 2003)[123] y los procesos en contra del Estado peruano ante la CIDH, obligando al Poder Ejecutivo promulgar el criticado D. Legislativo N°927 (2003), dándole a los condenados por el delito de terrorismo ciertos beneficios como redención de pena por trabajo y educación, y la liberación condicional[124].

La entrada en vigor de la Ley N°29423 (2009) derogó el problemático D. Legislativo N°927, estableciendo una vez más que los sentenciados por terrorismo y/o traición a la patria, no podían acogerse a los beneficios que diera la norma derogada, impidiendo así mecanismos de acceso anticipado a su libertad. Todos estos cambios marcaron un antes y un después en regulación en materia de terrorismo, dejando en claro que el Perú tenía una regulación antiterrorista que atentaba contra derechos y principios constitucionales, también consagrados en instrumentos internacionales. Toda esta parafernalia fue la que ocasionó la liberación de Lori Berenson, temida cabecilla del MRTA y que fue sentenciada n 1995 a cadena perpetua, sentencia que se revocó a pedida de la CIDH por considerar que esta era violatoria a sus propios derechos.

Esto nos debe servir de antecedente. No podemos cometer los mismos errores en la formulación de la Ley especial contra el ciberterrorismo. Tenemos los suficientes sustentos estadísticos, así como reportes nacionales e internacionales que demuestran que el terrorismo es una amenaza que pone en peligro a la población general de nuestra nación. Así mismo, tenemos reportes que permiten explicar el peligro que existe cuando se fusiona esta figura con las tecnologías e Internet y da paso al ciberterrorismo, dando en claro que es un peligro para la sociedad.

Adicional sustento mi posición en la teoría del **«Triángulo colaborativo»** (JAKOBS, 1983), planteando y aceptando a los ciberterroristas como enemigos de nuestra sociedad a quienes debemos combatir con la coacción. En su libro de 2003 plasma la opinión de tres personajes de la historia universal para sustentar aún más su posición. En ese sentido, cita a Rousseau quien afirma que **«al culpable se le hace morir más como enemigo que como ciudadano»**[125]; a su vez, Fichte establece que **«quien abandona el contrato ciudadano en un punto en el que en el contrato**

[122] Cfr. D. Legislativo N°654 (1991); D. Ley N°25475 (1992); D. Ley N°25744 (1992); D. Ley N°25916 (1992)
[123] Se declara inconstitucional el D. Ley N°25475 (1992).
[124] A este beneficio solo podía acogerse aquellos condenados que hayan cumplido ¾ de la pena impuesta.
[125] JAKOBS, Günther & CANCIO MELIÁ, Manuel (2003). *Derecho penal del ciudadano y derecho penal del enemigo*. En **«Derecho penal del enemigo»**. Pp. 27. Madrid, España. Editorial Thomsom Civitas.

se contaba con su prudencia, sea de modo voluntario o por imprevisión, en sentido estricto pierde todos sus derechos como ciudadano y como ser humano, y pasa a un estado de ausencia completa de derechos (…) a falta de personalidad, la ejecución criminal no es una pena, sino sólo instrumento de seguridad»[126]; y, finalmente, Kant se pronunciaría alegando que **«quien no participa en la vida en un estado comunitario-legal debe irse, no hay que tratarlo como persona, sino que se le puede tratar como un enemigo»**[127]. La visión, fundamentada en la filosofía política de las teorías contractualistas del Estado, es clara, pues quien no cumple con el contrato social debe ser tratado como un no ciudadano; es decir, como un enemigo.

Si nuestra futura norma es blanda en la lucha contra esta peligrosa figura, se está abriendo una puerta a favor de la defensa criminal, la corrupción y los nulos intereses por el bienestar de la ciudadanía. Si bien es labor del Juez el pronunciamiento sobre la pena a imponer, si no se le da las armar correctas, de nada vale su función como impartidor de justicia.

4.4.2. *Jueces sin rostro*

Si bien en 2005 la CIDH determinara que la figura de los jueces sin rostro viola el debido proceso, no podemos negar que durante los años 90s, la medida que instaurara el gobierno del expresidente Alberto Fujimori fue una respuesta necesaria ante el impedimento de procesar a los acusados del delito de terrorismo, por las fuertes amenazas públicas y privadas que recibían los magistrados.

El rescate de esta figura procesal es una alternativa que, esta vez, deberá ser plasmada de manera correcta en nuestra norma. La reforma penal nos coloca en un nuevo proceso de aprendizaje, capacitación y acción para jueces y fiscales, que han mejorado su trabajo durante la implementación de este proyecto de reestructuración penal. Es momento de darles mejores armas legislativas y solamente establecer esta medida para la lucha contra figuras como el terrorismo y ciberterrorismo.

E 2016, la CNDH reconoció que en México debe analizarse instaurar la presencia de los jueces sin rostro para los procesos de delitos contra el narcotráfico, buscando la integridad y protección de los magistrados. El Perú puede ir por el mismo camino, solo debe sustentar correctamente por qué necesita de este tipo de jueces y qué ventas traería a un proceso de este tipo. Todo ello debe queda por escrito y estipulado en el proyecto de Ley especial en el que se deberá trabajar.

[126] **Ibid.**
[127] **Ibid**. Pp. 31

4.4.3. *Muerte civil*

Se entiende por muerte civil a **«aquella situación jurídica en que, a una persona, aún en vida, se le despoja de sus derechos civiles y políticos»**. En palabras simples, una persona que es declara muerto civilmente no podría adquirir ni derechos ni obligaciones, quedando totalmente lejos de la protección del Estado; impidiendo a su vez la contracción de nupcias, celebración de contratos, entre otros derechos.

Esta alternativa debe darse si es que la categoría de máximo de la pena no pueda imponerse por algún motivo. Recordemos que hay procesados por terrorismo pertenecientes a SL que solo fueron sentenciados a 20 años y que están próximos a ser liberados, a diferencia de otros miembros de la misma organización como los principales cabecillas quienes cumplen condena de cadena perpetua. Existe una delgada línea que no nos asegura que la finalidad de reformación y reinserción a la sociedad se haya cumplido. Para estas personas, o, mejor dicho, para los ciberterroristas que puedan ser sentenciados de la misma manera, el hecho de agregar la muerte civil a su sentencia una vez salgan de las cárceles, es una manera dura pero certera de asegurar la seguridad en el Perú.

Debemos reconocer que nuestro sistema penitenciario es deficiente. Más que cumplir una sanción correctiva, parece cumplir una especie de especialización en el mundo del hampa. Es cierto decir que no todos los criminales corren el mismo riesgo, algunos logran pagar su deuda con la sociedad; pero es la ciudadanía quien percibe más al criminal nuevamente peligroso que al criminal reformado. Una vez reinsertados en la sociedad, los ex convictos recuperan sus derechos como ciudadanos, y es el mismo caso con los terroristas que saldrán en libertad o con los futuros ciberterroristas que llegarían a procesarse y cumplan su tiempo en la cárcel. Es preferible estar preparados ante la amenaza que experimentar con el beneficio de la duda. Indispensable aplicar la sanción de muerte civil al momento en que se dicte la sentencia; con lo que también deberá informarse a la población sobre su estado de civilmente muerto, y que la misma colabore con el cumplimiento de esta sanción una vez sea liberado.

4.4.4. *Prohibición del uso de tecnologías e ingreso a Internet*

Igualmente, expuesta en el *OAS-First Cyber Security Symposium*, el combinar esta alternativa con la muerte civil nos da una propuesta no solamente efectiva, sino drástica y necesaria. Si bien la muerte civil otorga una supresión al campo de acción de ex presidiario —dado por entendido que ya cumplió su sentencia—, eso no limita que pueda tener acceso a tecnología e Internet en su proceso de reinversión; es más, me atrevo a decir que seguirá teniendo ese acceso en el reclusorio donde sea designado. Si no hemos entendido que estos dos elementos son parte del cuerpo y mentalidad del ciberterrorista, no hemos aprendido nada de esta investigación.

Es indispensable que el juzgado por ciberterrorismo no pueda adquirir —por ningún método y bajo ningún concepto— acceso a Internet y tecnologías, pues estos serán utilizados como armas o medio de comunicación para con sus secuaces —de tenerlos—. De producirse esta figura, deberá ser sancionado una vez más. De igual forma, misma sanción deberá recibir todo aquel que le brinde ayuda para tener acceso a estos medios.

En la tesis de 2014 se contó con la colaboración de Cristian Amicelli, especialista en ciberseguridad de MKIT, reconocida empresa de ciberseguridad argentina, explicando que, si un ciberdelincuente atacó una vez un sistema, si tiene la oportunidad, lo volverá a hacer, por un instinto de demostrar poder o simplemente exposición ante la comunidad. Podría decirse que está dentro de sus patrones y es una conducta que no se podrá evitar.

Si bien la prohibición del uso de tecnologías e ingreso a Internet puede ser considerada una medida drástica y violatoria de DD.HH. como el acceso a la información, la historia criminal peruana nos ha enseñado que cada vez que se libera a un delincuente, este reincide en sus conductas y pone a una vez más en peligro a la población. Es por ello por lo que esta medida es preventiva en todo sentido. No le otorguemos un arma a aquel que sabe manejarla. Aquí, una vez más, ingresa la correcta legislación en la que se debe trabajar, la misma que priorice a la sociedad y la seguridad de la nación como los principales elementos a defender ante la figura del ciberterrorismo.

4.5. Reflexiones finales

El Perú es un país en constante crecimiento económico, un país que busca la estabilidad política y la seguridad de su nación; pero, su talón de Aquiles despreciado son los ciberdelitos, la mayor vulnerabilidad que hace del país un blanco fácil para las amenazas cibernética y una posible ciberguerra, un país que parece estancado solo en temas secundarios y no quiere aceptar la visión obligada que va teniendo cada país de la región y el mundo, que es la adaptación al mundo de la tecnología y la interconexión universal gracias a Internet. Tenemos mucho que aprender y muchos que trabajar en el transcurso de los años. Desde la publicación del Global Trends 2030 se recomendaba a los países prepararse en los próximos cinco años para hacer frente al ciberterrorismo, algo que no sucedió en nuestro país, pero que ya muchos países del mundo vienen discutiendo.

Debemos aceptar la dura realidad y afirmar que, por alguna extraña razón, no estamos listos para el cambio y no parce ser prioritario para nuestros legisladores. Cada día la criminalidad va avanzando y el país pretende enfrenta a esta corriente con leyes no funcionales y con códigos ahora modificados, pero bajo sombras de mundos de fantasía. Si antes pretendíamos luchar con códigos originarios de los años 80, ahora luchamos sin guía y sin conciencia de lo que sucede en el mundo. Todavía nos queda un par de puertas que abrir y cerrar, pero es un trabajo duro y

de mucha colaboración entre muchos sectores, entre nuestros propios *multistakeholders*.

Concluyo el presente trabajo solicitando que este sirva para futuras investigaciones en el campo y que sea tomado con conciencia tanto por el sector político como académico y todos aquellos que quieran aportar un grano de arena en la lucha contra el ciberterrorismo. Este es el estabón más débil, el legislativo, el de la escuela de derecho, el de la academia jurídica. Es momento de adaptarnos a la cadena evolutiva y dejar de ser parte de una visión Estatal que no quiere aceptar la peligrosidad de ciertas figuras ni verlas con seriedad. Que el Derecho sea una vez más el eje del cambio y la sostenibilidad social. Que el Derecho sea una vez más la rama que ponga en discusión muchos aspectos negativos de la sociedad y que proponga el cambio, por el bien de esta y de las generaciones que vengan.

CAPÍTULO VI
REFERENCIAS

1. Referencias bibliográficas

BRAMONT–ARIAS TORRES, Luis (1997). **«El Delito Informático en el Código Penal Peruano»**. Pp.27. Fondo Editorial de la Pontificia Universidad Católica del Perú. Lima, Perú.

CANO PAÑOS, Miguel Ángel (2013). **«Tratamiento del fenómeno terrorista en el Derecho Penal»**. Lima, Perú. ARA Editores E.I.R.L.

DAVARA RODRÍGUEZ, Miguel Ángel (2008). **«Manual de Derecho Informático»**. Pamplina, España. Editorial Thomson–Aranzadi.

HIGGINS, Rosalyn & FLORY, Maurice (1997). **«Terrorism and International Law»**. Londres, Inglaterra. Editorial Routledge.

JAKOBS, Günther & CANCIO MELIÁ, Manuel. (2003). **«Derecho penal del enemigo»**. Madrid, España. Editorial Thomsom Civitas.

JIMÉNEZ BACA, Benedicto (2000). **«Inicio, Desarrollo y Ocaso del Terrorismo en el Perú. El ABC de Sendero Luminoso y el MRTA ampliado y comentado – Tomo I»**. Lima, Perú. Editorial Sanki.

JIMÉNEZ BACA, Benedicto (2000). **«Inicio, Desarrollo y Ocaso del Terrorismo en el Perú. El ABC de Sendero Luminoso y el MRTA ampliado y comentado – Tomo II»**. Lima, Perú. Editorial Sanki.

NATO Science for Peace and Security Series: Human and Societal Dynamics (2008). **«Responses to Cyber Terrorism»**. Vol. 34. IOS Press.

NATO Science for Peace and Security Series: Information and Communication Security (2015). **«Terrorist Use of Cyberspace and Cyber Terrorism: New Challenges and Responses»**. Vol. 42. IOS Press.

OSSORIO, Manuel (2003). **«Diccionario de Ciencias Jurídicas, Políticas y Sociales»**. 23° Edición actualizada, corregida y aumentada por Guillermo Cabanellas de las Cuevas. Buenos Aires, Argentina. Editorial Heliasta S.R.L.

SANTIVÁÑEZ MARIN, Juan José M. (2013). **«Seguridad Ciudadana. Estrategias para combatir la Inseguridad Ciudadana»**. Lima, Perú. AFA Editores Importadores S.A.

TAYLOR, Robert W.; FRITSCH, Eric J. & LIEDERBACH, John (2014). **«Digital Crime and Digital Terrorism»**. EE. UU. Pearson Editorial.

TÉLLEZ VALDÉZ, Julio (2009). **«Derecho Informático»**. México DF, México. McGRAW-HILL/INTERAMERICANA EDITORES S.A.

TIEDEMANN, Klaus (1985). **«Poder económico y delito: introducción al derecho penal económico y de la empresa»**. Barcelona, España. Editorial Ariel.

VERTON, Dan (2004). **«Black Ice: La amenaza invisible del terrorismo»**. Madrid, España. McGraw Hill / Interamericana de España.

2. Referencias hemerográficas

AKATI-UDI, Tega (2015). **«Combating the growing threat of cyber terrorism»**. Special Conference 2 on International Cooperation. Conferencia llevada a cabo en Model United Nations International School of The Hague 2015 | XXV Annual Session.

ALKHOURI, Laith & KASSIRER, Alex (2016). **«Tech for Jihad: Dissecting Jihadists' Digital Toolbox»**. Flashpoint.

ALONSO, Chema. Maligno Alonso. 15 de abril de 2013. **«Mundo Hacker en Discovery MAX – Capitulo 3: Ciberguerra»**.

AL-RAWI, Ahmed (2016). **«Video games, terrorism, and ISIS's Jihad 3.0»**. Terrorism and Political Violence Journal, Vol. 29, Issue 6. Pp. 1-21. 2017, De Taylor & Francis online Base de datos.

ARGENTINA: **«Ley N°26.388 del 25 de junio de 2008 – Texto de la ley de reforma del Código Penal en materia de Delitos Informáticos»**.

ARROYO VÁZQUEZ, Natalia (2007). **«¿Web 2.0? ¿Web social? ¿Qué es eso?»**. Revista Educación y Biblioteca, núm. 161. Madrid, España.

BANCO INTERAMERICANO DE DESARROLLO (2016). Documento para discusión N°IDB-DP-457 **«Experiencias avanzadas en políticas y prácticas de ciberseguridad: Panorama general de Estonia, Israel, República de Corea y Estados Unidos»**. Obra sujeta a licencia CreativeCommons IGO 3.0 Reconocimiento-NoComercial-SinObrasDerivadas (CC-IGO 3.0 BY-NC-ND).

BANCO INTERAMERICANO DE DESARROLLO Y LA ORGANIZACIÓN DE ESTADOS AMERICANOS (2016). Documento **«Ciberseguridad: ¿Estamos preparados en América Latina y el Caribe?»**. Obra sujeta a licencia CreativeCommons IGO 3.0 Reconocimiento-NoComercial-SinObrasDerivadas (CC-IGO 3.0 BY-NC-ND).

BOLIVIA: **«Ley N°164 del 8 de agosto de 2011 – Ley General de Telecomunicaciones, Tecnologías de Información y Comunicación»**.

BONILLA LEONARDO, José Martín. (2013). **«Eficacia y Constitucionalidad del Derecho Penal del Enemigo»**. Revista Institucional de la Facultad de Derecho y Ciencia Política - Universidad Nacional de San Cristóbal de Huamanga, N°9, pp. 67-76.

CHILE: **«Ley N°19223 del 07 de junio de 1993 – Ley que Tipifica Figuras Penales relativas a la Informática»**.

CHARLES, Alec (2009). **«Playing with one's self: notions of subjectivity and agency in digital games»**. Eludamos: Journal for Computer Game Culture, Vol. 3, Issue 2. Pp. 281-294. 2017, De Eludamos Base de datos.

CHICHARRO LÁZARO, Alicia. (2009). **«La labor legislativa del Consejo de Europa frente a la utilización de Internet con fines terroristas»**. IDP: Revista de Internet, Derecho y Política. N°9. Pp. 1-14.

COLOMBIA: **«Ley N°1273 del 05 de enero del 2009 – Ley que modifica el Código Penal, creando un nuevo bien jurídico tutelado denominado "de la protección de la información y de los datos»**.

COLLIN, Barry - Institute for Security and Intelligence (1984). **«The future of cyberterrorism: Where the physical and virtual worlds converge»**. 11th Annual international symposium on criminal justice issues. Congreso llevado a cabo en California, EE. UU.

CONSTITUCIÓN POLÍTICA DEL PERÚ. Año 1993.

COMITÉ INTERAMERICANO CONTRA EL TERRORISMO. **«Declaration strengthening cyber-security in the americas»**. EE.UU., 7 de marzo de 2012. Documento CICTE/DEC.1/12 rev. 1

COMITÉ INTERAMERICANO CONTRA EL TERRORISMO. **«Plan de trabajo para 2013 del comité interamericano contra el terrorismo»**. EE.UU., 8 de marzo de 2013. Documento CICTE/doc.2/13 rev.1

COMITÉ INTERAMERICANO CONTRA EL TERRORISMO. **«Proyecto de plan de trabajo para 2017 del comité interamericano contra el terrorismo»**. EE.UU., 17 de febrero de 2017. Documento CICTE/doc.6/17

COMITÉ INTERAMERICANO CONTRA EL TERRORISMO. **«Informe sobre la implementación del plan de trabajo del 2016 del comité interamericano contra el terrorismo»**. EE.UU., 6-7 de abril de 2017. Documento CICTE/doc.5/17.

COMITÉ INTERAMERICANO CONTRA EL TERRORISMO. **«Report of the executive secretariat of CICTE»**. EE.UU., 6-7 de abril de 2017. Documento CICTE/INF.4/17 corr. 1

COMITÉ INTERAMERICANO CONTRA EL TERRORISMO. **«Resolución: Establecimiento de un grupo de trabajo sobre medidas de fomento de cooperación y confianza en el ciberespacio»**. EE.UU., 7 de abril de 2017. Documento CICTE/RES.1/17.

CONVENCIÓN INTERAMERICANA CONTRA EL TERRORISMO. Barbados, 3 de junio de 2002. Documento AG/RES. 1840 (XXXII-O/02).

COOPERACIÓN HEMISFÉRICA PARA PREVENIR, COMBATIR Y ELIMINAR EL TERRORISMO. Argentina, 7 de junio de 1999. Documento AG/RES. 1650 (XXIX-O/99).

COSTA RICA: **«Ley N°9048 del 10 de julio de 2012 – Reforma de varios artículos y modificación de la Sección VIII denominada "Delitos Informáticos y Conexos", de Título VII del Código Penal»**.

COUNCIL OF EUROPE / CONSEIL DE L'EUROPE. **«Convenio sobre la Ciberdelincuencia (Budapest, 23.XI.2001)»**. Serie de Tratados Europeos N°185. Budapest, Hungría. 23 de noviembre de 2001.

COUNTER-TERRORISM IMPLEMENTATION TASK FORCE (2009). Documento **«Report of the Working Group on Countering the Use of the Internet for Terrorist Purposes»**.

CRUZ VALENCIA, Galvy Ilvey (2012). **«Hacktivismo: ¿delito o comunicación ciudadana?»** Revista Seguridad. Cultura de prevención para ti. 12. pp. 26-31.

DIARIO EL COMERCIO. Sección Política. **«Los delitos informáticos serán castigados con pena de cárcel»**. Artículo publicado el 13 de septiembre de 2013. Lima – Perú.

DIRECCIÓN GENERAL DE LA POLICÍA Y LA GUARDIA CIVIL - DIRECCIÓN ADJUNTA OPERATIVA JEFATURA DE INFORMACIÓN DEL MINISTERIO DEL INTERIOR DE ESPAÑA (2010). **«Sesión tecnológica 6 - Caso de la seguridad en la red: ciberterrorismo»**. En J. RIVERO LAGUNA (Presidencia). XII Congreso DINTEL profesionales IT 2010 TESIC (Tecnologías y Seguridad en Infraestructuras Críticas). Congreso llevado a cabo en Madrid, España.

ESTADOS UNIDOS DE AMERICA: **«Acta Federal de Abuso Computacional (18 U.S.C. Sec. 1030) de 1994, que modifica el Acta de Fraude y Abuso Computacional de 1986»**.

GORDON, Sarah & FORD, Richard (2003). Documento White Paper **«Cyberterrorism?»**. Symantec Security Response. Copyright © 2003 Symantec Corporation. All rights reserved.

GORDON, Sarah (2003). Documento White Paper **«Cyberterrorism and the Home User»**. Symantec Security Response. Copyright © 2003 Symantec Corporation. All rights reserved.

FIDLER, David P. (2016). **«Cyberspace, Terrorism and International Law»**. Journal of Conflict and Security Law, Volume 21, Issue 3. Pp. 475–493. 2017, De Oxford Academic Base de datos.

FIDLER, David P.; PREGENT, Richard & VANDURME, Alex. (2013). **«NATO, Cyber Defense, and International Law»**. 4 St. John's Journal of International & Comparative Law. Pp. 1-25. 2017, De Maurer School of Law: Indiana University (Digital Repository) Base de datos.

FURNELL, S.M. & WARREN, M.J. (1999). **«Computer hacking and cyber terrorism: the real threats in the new millennium?»**. Computers & Security Journal, Volume 18, Issue 1, Pp. 28-34. 2017, De ScienceDirect Base de datos.

GUTIÉRREZ, Angélica (2012). **«Cómo el terrorismo islamista usa Internet»**. Quadernos de criminología: revista de criminología y ciencias forenses, N°19, Pp. 8-13. 2017, de DIALNET Base de datos.

HOLANDA: **«Ley de Delitos Informáticos del 01 de marzo de 1993»**.

INCIBE/BOE (2016). **«Código de Derecho de la ciberseguridad»**. Edición actualizada al 27 de septiembre de 2017.

INTERPOL (2017). **«Global crime strategy»**. [Summary].

INTERPOL (2017). **«Global strategy on organized and emerging crime»**. [Summary].

INTERPOL (2017). **«Global counter-terrorism strategy»**. [Summary].

INTERPOL (2017). **«Cybercrimen: Future-oriented policing projects»**.

SWIMMER, Morton (2010). **«Cyberterrorism. Oh Really?»**. Virus Bulletin. Recuperado de: https://www.virusbulletin.com/uploads/pdf/conference_slides/2010/Swimmer-VB2010.pdf

SYMANTEC (2016). Documento **«ISRT 2016»**. Vol.21**.** Copyright © 2016 Symantec Corporation. All rights reserved.

SYMANTEC (2017). Documento **«ISRT 2017»**. Vol.21. Copyright © 2017 Symantec Corporation. All rights reserved.

MICROSOFT CORPORATION (2017). **«Microsoft Cyber Defense Operations Center: Strategy Brief»**. EE. UU.: Microsoft Corporation.

NAIK, Saheli (2017). **«A Biggest Threat to India – Cyber Terrorism and Crime»**. Journal of Research in Humanities and Social Science. Vol. 5, Issue 4. Pp. 27-30. 2017, De Quest Journals Base de datos.

NACIONES UNIDAS. **«12º Congreso de las Naciones Unidas sobre Prevención del Delito y Justicia Penal»**, A/CONF.213/L.6/Rev.2 (12 a 19 de abril de 2010).

NACIONES UNIDAS. **«13º Congreso de las Naciones Unidas sobre Prevención del Delito y Justicia Penal»**, A/CONF.222/L.6 (12 a 19 de abril de 2015).

OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE (2000). Documento **«Global Trends 2015: A dialogue about the future with Nongovernment experts»**.

OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE (2012). Documento **«Global Trends 2030: Alternative Worlds. A publication of the National Intelligence Council»**. ISBN 978-1-929667-21-5.

OFICINA DE LAS NACIONES UNIDAS CONTRA LA DROGA Y EL DELITO (2006). Documento **«Foro sobre el delito y la sociedad»**. Volumen 4, números 1 y 2, diciembre de 2004. Publicación de las Naciones Unidas. Impreso en Austria.

OFICINA DE LAS NACIONES UNIDAS CONTRA LA DROGA Y EL DELITO (2013). Documento **«El uso de internet con fines terroristas»**. Publicación de las Naciones Unidas. Impreso en Austria.

ORGANIZACIÓN DE ESTADOS AMERICANOS Y LA PRESIDENCIA DE LA REPÚBLICA DE MÉXICO (2017). Documento **«Hacia una estrategia nacional de ciberseguridad: Consolidación de las consultas a actores nacionales»**.

PABLO, Roberto & DE AZUMENDI, Lartaun (2013). **«¿Qué es el ciberespionaje y ciberterrorismo?»**. [podcast] La Noche.
Disponible en: http://www.cope.es/audios/noche/que-ciberespionaje-ciberterrorismo_340430 [Acceso 10 Mar. 2017].

PARAGUAY: **«Ley N°4439 – Ley que modifica y amplía varios artículos de la Ley N°1160/97 del Código Penal del 03 de octubre de 2011»**.

PAGET, François (2012). **«¿Hacktivismo – El ciberespacio: nuevo medio de difusión?»**. McAfee®.

PERÚ: **«Ley N°27309 del 15 de junio de 2000 – Ley que incorpora los Delitos Informáticos al Código Penal»**.

PERÚ: **«Proyectos Ley 034/2011-CR, 307/2011-CR y 1136/2011-CR. Proyectos que modifican lo regulado por la Ley N°27309»**.

PERÚ: **«Ley N°30096 del 23 de octubre de 2013 – Nueva Ley de Delitos Informáticos»**.

PERÚ: **«Ley N°30171 del 10 de marzo de 2014 – Nueva Ley de Delitos Informáticos»**.

PÉREZ, Jorge & OLMOS, Ana (2009). **«Introducción: Gobernanza de Internet»**. Investigación: Dossier TELOS. N°80.

POLICÍA NACIONAL DEL PERÚ. **«Historia de la División de Delitos de Alta Tecnología de la DIRINCRI (DIVINDAT)»**.

POLLITT, Mark - Federal Bureau of Investigation Laboratory (1997). **«CYBERTERRORISM - Fact or Fancy?»**. En National Institute of Standards and Technology, National Computer Security Center. Trabajo presentado en *20th National Information Systems Security Conference*. Pp. 285-289. Baltimore-MD, EE. UU. Proceedings of the 20th National Information Systems Security Conference.

PRESIDENCIA DEL GOBIERNO DE ESPAÑA (2013). **«Estrategia de ciberseguridad nacional»**.

RAPID7® (2017). **«National Exposure Index, 2017»**. Rapid7® Labs.

REDACCIÓN EL COMERCIO (2013). **«Los delitos informáticos serán castigados con pena de cárcel»**. Diario El Comercio, Pp. 13.

SÁNCHEZ MEDERO, Gema (2012). **«Ciberespacio y el crimen organizado, los nuevos desafíos del siglo XXI»**. Revista Enfoques, Vol. X - N°16, Pp. 71-87.

SARZANA, Carlo (1999). **«Criminalità e tecnología: Computer crime»**. Pp.53. Roma, Italia. Rassagna Penitenziaria e Criminología.

TÉLLEZ VALDÉS, Julio (1992). **«Terrorismo por computadora»**. Informática y Derecho: revista iberoamericana de derecho informático, N°1, pp. 177-184. 2017, De Google académico Base de datos.

TREND MICRO Y LA ORGANIZACIÓN DE ESTADOS AMERICANOS (2015). Documento **«Reporte de Seguridad Cibernética e Infraestructura Crítica de las Américas»**. Todos los derechos reservados © 2015 Trend Micro Incorporated & © OAS Secretariat for Multidimensional Security

TUNIS AGENDA FOR THE INFORMATION SOCIETY. Túnez, 18 de noviembre de 2005. Documento WSIS-05/TUNIS/DOC/6(Rev. 1)-E.

UNITED KINGDOM OF GREAT BRITAIN AND NORTHERN IRELAND (1990). **«Computar Misuse Act of 1990: chapter 18 - Arrangement of sections»**.

UNITED NATIONS: COUNTER-TERRORISM IMPLEMENTATION TASK FORCE (2011). Documento **« Countering the Use of the Internet for Terrorist Purposes - Legal and Technical Aspects»**.

VENEZUELA: **«Ley Especial contra los Delitos Informáticos de Venezuela del 30 de octubre de 2001»**.

WEIMANN, Gabriel (2004). **«Cyberterrorism: How Real Is the Threat?»** (Pp. 1-12). EE. UU. : United States Institute of Peace (USIP).

WIRTZ, Bernd W. & WEYERER, Jan C. (2016). **«Cyberterrorism and Cyber Attacks in the Public Sector: How Public Administration Copes with Digital Threats»**. International Journal of Public Administration, Vol. 40, Issue 13. Pp. 1085-1100. 2017, De Taylor & Francis online Base de datos.

YAHOO! GRUPOS – ESPAÑA. **«Correo cadena caso Pulp®!»** Publicado el 24 de noviembre de 2006. Recuperado de: http://es.groups.yahoo.com/group/Juanalarquinas/message/142

3. Referencias Electrónicas

ACHARYA, Subhojyoti (2007). **«Cyber Terrorism- The Dark Side of the Web World»**. 2017, del portal Legal Service India. Sitio web: http://www.legalserviceindia.com/article/l169-Cyber-Terrorism.html

AGENCE FRANCE PRESSE (2017) **«Ciberterrorismo, una amenaza latente para el mundo: Kaspersky»**. Del portal digital El Economista, sección *Ciberseguridad*. Sitio web: https://www.eleconomista.com.mx/tecnologia/Ciberterrorismo-una-amenaza-latente-para-el-mundo-Kaspersky-20170301-0054.html

AGENCIA EFE (2014). **«El ciberterrorismo es una actividad en continuo crecimiento»**. 2017, del portal El Espectador. Sitio web: https://www.elespectador.com/noticias/actualidad/el-ciberterrorismo-una-actividad-continuo-crecimiento-articulo-523789

AHN, JH (2016). **«Calls for anti-cyber terrorism bill resurface in South Korea»**. 2017, del portal NK News. Sitio web: https://www.nknews.org/2016/08/calls-for-anti-cyber-terrorism-bill-resurface-in-south-korea/

ANDREU, Jerónimo (2017). **«Yihadistas recurren a videojuegos para atraer a jóvenes»**. Del portal El Universal, sección *Mundo*. Sitio web: http://www.eluniversal.com.mx/articulo/mundo/2017/06/22/yihadistas-recurren-videojuegos-para-atraer-jovenes

ÁVILA-MOLINA, Oscar Noé. **ISOC Cybersecurity SIG**. 14 de septiembre de 2017. **«Webinar: ¿Esto es Ciberseguridad o Ciberdefensa? ¡No! Se trata de CiberInteligencia»**. Recuperado de https://www.youtube.com/watch?v=qWcPhbwMUKo

BALKHI, Syed (2014). **«25 Biggest Cyber Attacks In History»**. 2017, del portal List25, sección *History*. Sitio web: https://list25.com/25-biggest-cyber-attacks-in-history/

BENDEZÚ, Rider (2013). **«Advierten peligros de Ley de Delitos Informáticos»**. Del portal La República, sección *Política*. Sitio web: http://larepublica.pe/politica/742700-advierten-peligros-de-ley-de-delitos-informaticos

BENNETT, Brian (2015). **«CIA to create a digital spy division»**. 2017, del portal Los Angeles Times. Sitio web: http://beta.latimes.com/nation/nationnow/la-na-nn-cia-cyber-espionage-20150305-story.html

BREWSTER, Thomas (2012). **«NATO: Cyber Terrorism Not Yet A Real Threat»**. 2017, del portal Silicon, sección *Security*. Sitio web: http://www.silicon.co.uk/workspace/nato-cyber-terrorism-84942?inf_by=5a695346681db8ed248b4b50

BROWNE, Ryan (2017). **«NATO: We ward off 500 cyberattacks each month»**. Del portal CNN, sección *Politics*. Sitio web: http://edition.cnn.com/2017/01/19/politics/nato-500-cyberattacks-monthly/index.html

BUDD, Christopher (2016). **«Drawing the line: How cyber criminals' online tactics differ from terrorists'»**. 2017, de Trend Micro Blog. Sitio web: https://blog.trendmicro.com/drawing-the-line-how-cyber-criminals-online-tactics-differ-from-terrorists/

CALDERÍN, Juanfer & JIMÉNEZ, María (2016). **«Estados Unidos, Rusia o China presentan ventajas para el cibercrimen»**. 2017, del portal Observatorio Internacional de Estudios sobre Terrorismo (OIET). Sitio web: http://observatorioterrorismo.com/entrevistas/eeuu-rusia-y-china-son-paraisos-del-ciberterrorismo/

CAMP, Cameron (2011). **«Hack wireless industrial sensors in a few easy steps»**. 2017, del portal We Live Security, sección *Cybercrime*. Sitio web: https://www.welivesecurity.com/2011/08/09/hack-wireless-industrial-sensors-in-a-few-easy-steps/

CAMP, Cameron (2011). **«US Pentagon: it's official, military response to cyber attacks»**. 2017, del portal We Live Security, sección *Civil Rights*. Sitio web: https://www.welivesecurity.com/2011/11/21/us-pentagon-its-official-military-response-to-cyber-attacks/

CAMP, Cameron (2011). **«SCADA attacks gone crazy»**. 2017, del portal We Live Security, categoría *Blackhat*. Sitio web: https://www.welivesecurity.com/2011/11/21/scada-attacks-gone-crazy/

CANO, Luis (2014). **«De la guerra en los videojuegos a la yihad»**. 2017, del portal ABC internacional. Sitio web: http://www.abc.es/internacional/20141127/abci-violencia-videojuegos-terrorismo-guerra-201411262047.html

CARTER, Chelsea J. (2014). **«Video shows ISIS beheading U.S. journalist James Foley»**. Del portal CNN. Sitio web: http://edition.cnn.com/2014/08/19/world/meast/isis-james-foley/index.html

CASPIAN KANG, Jay (2014). **«ISIS's Call of Duty»**. 2017, del portal The New Yorker, sección Elements. Sitio web: https://www.newyorker.com/tech/elements/isis-video-game

CENTRAL INTELLIGENCE AGENCY. Sitio web: https://www.cia.gov/

CHAYA, George (2017). **«Avanza la batalla legal contra la publicidad del terrorismo en internet»**. Del portal Infobae. Sitio web: https://www.infobae.com/america/mundo/2017/07/02/avanza-la-batalla-legal-contra-la-publicidad-del-terrorismo-en-internet/

«Ciberterrorismo: Una amenaza gubernamental a la privacidad». Recuperado de: http://www.paginasprodigy.com/tesisdehackers/cibercap1.html#ciberterrorismo

CONEXIÓN ESAN (2015). **«Web 3.0: diez características que te permitirán identificarla»**. De "Sección apuntes empresariales / tecnologías". Sitio web: https://www.esan.edu.pe/apuntes-empresariales/2015/05/web-3-diez-caracteristicas-que-te-permitiran-identificarla/

CROMPTON, Paul (2014). **«Grand Theft Auto: ISIS? Militants reveal video game»**. 2017, del portal Al Arabiya English, sección *Variedad*. Sitio web: http://english.alarabiya.net/en/variety/2014/09/20/Grand-Theft-Auto-ISIS-Militants-reveal-video-game.html

CUMBRE DE LAS AMERICAS (2005). **«Archivo de las Reuniones en el Área de la Lucha Contra Terrorismo»**. 2017. Sitio web: http://www.summit-americas.org/Quebec_Summit/Quebec-hem-security/Old%20Back%20up/hem-security-archives-terrorism-span.htm

DEL BARRIO, Juan Martin (2012). **«La ONU ve las redes sociales como vía de captación de terroristas»**. 2017, del portal El País, sección *Tecnología*. Sitio web: https://elpais.com/tecnologia/2012/10/23/actualidad/1350980383_717529.html

DI NOLFI, Salvatore (2017). **«Hacker y cracker, diferencias de significado»**. De FundéuBBVA. Sitio web: http://www.fundeu.es/recomendacion/hacker-y-cracker-diferencias-de-significado/

ELECONOMISTA.ES (2010). **«China lanza un Ciberataque contra una teleco australiana por error»**. 2014, del portal EcoDiario.es, sección *Telecomunicaciones y Tecnología*. Sitio web: http://ecodiario.eleconomista.es/telecomunicaciones-tecnologia/noticias/2061591/04/10/China-lanza-un-ciberataque-contra-una-teleco-australiana-por-error.html

ESCOBAR, Ana Cecilia (2012). **«¿Qué es el hacktivismo?»**. 2017. Del portal Daily Trend, sección *Radar*. Sitio web: http://www.dailytrend.mx/radar/101-que-es-el-hacktivismo#pageview-1

FISHER, Jonathan (2015). **«A former CIA chief says other governments could launch crippling computer attacks on the US»**. 2017. Del portal Business Insider. Sitio web: http://www.businessinsider.com/former-cia-chief-cyberterrorism-on-mind-2015-5

FORBES STAFF (2015). **«Las 10 naciones mejor preparadas contra ciberataques»**. Del portal Forbes México, sección Tecnología. Sitio web: https://www.forbes.com.mx/las-10-naciones-mejor-preparadas-contra-ciberataques/

FUSCALDO, Donna (2010). **«Protecting Small Businesses from Cyber Terrorism»**. 2017, del portal Fox News. Sitio web: http://www.foxbusiness.com/features/2010/10/08/protecting-small-businesses-cyber-terrorism.html

GARCÍA, Jaime & CALDERÓN, Julio (2003). **«China lanza un Ciberataque contra una teleco australiana por error»**. 2017, del portal El Salvador, sección *Nacionales*. Sitio web: http://archivo.elsalvador.com/noticias/2003/1/24/nacional/nacio8.html

GASPAR, Isabel M. (2017). **«Invertir contra el ciberterrorismo será una prioridad»**. Del portal El Universal. Sitio web: http://www.eluniversal.com.mx/articulo/cartera/economia/2017/06/30/invertir-contra-el-ciberterrorismo-sera-una-prioridad

GOBIERNO DE ESPAÑA - Ministerio de Asuntos Exteriores y de Cooperación. **«Ciberseguridad y cooperación Internacional»**. Información detallada en el documento recuperado: http://www.exteriores.gob.es/Portal/es/PoliticaExteriorCooperacion/Ciberseguridad/Paginas/Ciberseguridad-y-Cooperaci%C3%B3n-Internacional.aspx

GONZÁLEZ, Alberto (2015). **«Sony responde sobre el uso de PlayStation 4 como vía de comunicación por los terroristas de París»**. De Vandal. Sitio web: http://www.vandal.net/noticia/1350670677/sony-responde-sobre-el-uso-de-playstation-4-como-via-de-comunicacion-por-los-terroristas-de-paris/

GREENE, Tim (2016). **«Trend Micro: 6 most popular homebrewed terrorist tools»**. 2017, de Network World, sección *Security*. Sitio web: https://www.networkworld.com/article/3065213/security/trend-micro-6-most-popular-homebrewed-terrorist-tools.html

GROSS, Grant (2012). **«UN: More international cooperation needed to fight cyberterrorism»**. 2017, Computer World. Sitio web: https://www.computerworld.com/article/2492864/cybercrime-hacking/un--more-international-cooperation-needed-to-fight-cyberterrorism.html

GUARDIOLA, José Antonio. **Corporación de Radio y Televisión Española (RTVE)**. 4 de octubre de 2012. **«Amenaza Cyber»**. Recuperado de: http://www.rtve.es/alacarta/videos/en-portada/portada-amenaza-cyber/1543800/

GUERRA, Miguel (2012). **«Declaración de ciberdefensa del Perú y la informática gubernamental»**. Del portal digital Peru21, Sección *Atajos* web. Sitio web: http://blogs.peru21.pe/atajosweb/2012/04/declaracion-de-ciberdefensa-del-peru-informatica-gubernamental.html

HALL, Matthew (2014). **«"This is our Call of Duty": How ISIS is using video games»**. 2017, del portal Salon. Sitio web: https://www.salon.com/2014/11/01/this_is_our_call_of_duty_how_isis_is_using_video_games

HARLEY, David (2009). **«The Truth About Cybercrime»**. 2017, del portal We Live Security, sección *Cybercrime*. Sitio web: https://www.welivesecurity.com/2009/10/08/the-truth-about-cybercrime/

HATTEM, Julian (2015). **«CIA chief: Cyber terror is the future»**. 2017, del portal The Hill. Sitio web: http://thehill.com/policy/technology/235646-cia-chief-cyber-terror-is-the-future

HEATH, Nick (2008). **«Nato: Cyber terrorism "as dangerous as missile attack"»**. 2017, de Computer Crime Research Center. Sitio web: http://www.crime-research.org/news/10.03.2008/3241/

HUERTAS GRANADA, Yenalia (2016). **«La captación de terroristas a través de internet es un riesgo latente»**. 2017, de Granada Hoy. Sitio web: http://www.granadahoy.com/granada/captacion-terroristas-traves-internet-latente_0_1001300178.html

INCIBE. 2017. Sitio Web: https://www.incibe.es/

INI, Federico. **Canal de Federico INI**. 24 de enero de 2007. **«Ciberterrorismo, ¿Mito o Realidad?»**. Reportaje perteneciente al programa televisivo "*Informe Central*", conducido por Rolando Graña. Recuperado de: http://www.youtube.com/watch?v=h4a_QIwbRjE

INTERNET SOCIETY. **«Breve historia de internet»**. 2017, de Internet Society. Sitio web: https://www.internetsociety.org/es/breve-historia-de-internet/

INTERNET SOCIETY (2016). **«Informe de políticas: Gobernanza de Internet»**. Recuperado del sitio web: https://www.internetsociety.org/es/policybriefs/internetgovernance

INTERPOL (2017). **« Los peligros del terrorismo y la ciberdelincuencia para la seguridad en Europa, temas centrales de una reunión de INTERPOL»**. De Interpol, *Centro de Prensa*. Sitio web: https://www.interpol.int/es/Centro-de-prensa/Noticias/2017/N2017-064

INTERPOL (2017). **«INTERPOL to highlight need for military to police terrorism data flow at Global Coalition meeting»**. De Interpol, *Centro de Prensa*. Sitio web: https://www.interpol.int/es/News-and-media/News/2017/N2017-091

INTERPOL (2017). **«Terrorism intelligence shared via INTERPOL's Project Kalkan strengthens global 'early warning system'»**. De Interpol, *Centro de Prensa*. Sitio web: https://www.interpol.int/es/News-and-media/News/2017/N2017-090

INTERPOL. 2017. Sitio web: https://www.interpol.int/

ISLA ISUIZA, Ronny (2012). **«Webs peruanas son el paraíso para hackers, según experto en ciberseguridad»**. Del portal El Comercio, sección *Tecnología*. Sitio web: http://archivo.elcomercio.pe/tecnologia/actualidad/webs-peruanas-son-paraiso-hackers-segun-experto-ciberseguridad-noticia-1399830

JOYE, Christopher (2013). **«Cyber-attackers penetrate Reserve Bank networks»**. 2017, de The Australian Financial Review. Sitio web: http://www.afr.com/news/economy/monetary-policy/cyberattackers-penetrate-reserve-bank-networks-20130310-ji534

JOHNSON, Bobbie (2008). **«Nato says cyber warfare poses as great a threat as a missile attack»**. 2017, del portal The Guardian. Sitio web: https://www.theguardian.com/technology/2008/mar/06/hitechcrime.uksecurity

KRAMER, Albert (2016). **«Terroristen zijn als journalisten – Albert Kramer»**. 2017, de Deredactie, categoría *Opinión*. Sitio web: http://deredactie.be/cm/vrtnieuws/opinieblog/opinie/1.2683998#

KRAMER, Albert (2016). **«Cybercriminals and terrorists are more similar than we think»**. 2017, de Trend Micro Blog. Sitio web: http://blog.trendmicro.be/cybercriminals-terrorists-similar-think/

LESACA, Javier (2015). **«On social media, ISIS uses modern cultural images to spread anti-modern values»**. 2017, del portal Brookings, sección *Techtank* (technology policy) Sitio web: https://www.brookings.edu/blog/techtank/2015/09/24/on-social-media-isis-uses-modern-cultural-images-to-spread-anti-modern-values/

LIPOVSKY, Robert & CHEREPANOV, Anton (2014). **«El troyano BlackEnergy ataca a una planta de energía eléctrica en Ucrania»**. 2017, del portal We Live Security (Español), categoría *Investigaciones*. Sitio web: https://www.welivesecurity.com/la-es/2016/01/05/troyano-blackenergy-ataca-planta-energia-electrica-ucrania/

LYONS, Jhon (2017). **«Guerra cibernética y ciberterrorismo»**. Texto de Fundación innovación Bankinter/ICSPA. Del portal El Mundo. Sitio web: http://www.elmundo.es/economia/2017/03/28/58da300a22601d4a3e8b4649.html

MÁS VALE TARDE. **Canal de laSexta Noticias**. 17 de enero de 2015. **«Así se comunican mediante videojuegos los terroristas del ISIS»**. Reportaje perteneciente al programa televisivo "*Más Vale Tarde*". Recuperado de: https://www.youtube.com/watch?v=pw-UYPIAPzY

McLEAN, Doug (2009). **«Combatting Cyber-terrorism Requires We Play Defense AND Offense»**. 2017, de Symantec Official Blog. Sitio web: https://www.symantec.com/connect/blogs/combatting-cyber-terrorism-requires-we-play-defense-and-offense

MICÓ, J. L. (2012). **«La ONU insta a los gobiernos a mejorar la lucha contra el ciberterrorismo»**. 2017, del portal La Vanguardia. Sitio web: http://www.lavanguardia.com/internacional/20121027/54353564247/onu-gobiernos-lucha-contra-ciberterrorismo.html

MICROSOFT CORPORATION (2001). **«Thwarting Cyber Terrorism»**. 2017, del portal Microsoft. Sitio web: https://www.microsoft.com/issues/essays/2001/12-04cyberterrorism.mspx

MICROSOFT CORPORATION (2017). **«Closing the circle on digital crime»**. Del portal Microsoft. Sitio web: https://news.microsoft.com/europe/features/closing-the-circle-on-digital-crime/

MOIME, Dipolelo (2016). **«Cyber attacks on the rise in South Africa»**. 2017, del portal African Brand Link. Sitio web: http://africanbrandlink.com/cyber-attacks-rise-south%C2%A0africa

MORALES, Yolanda (2017). **«Ciberterrorismo, riesgo identificado por el WEF desde 2007 y subrayado este año»**. Del portal El Economista. Sitio web: https://www.eleconomista.com.mx/opinion/Ciberterrorismo-riesgo-identificado-por-el-WEF-desde-2007-y-subrayado-este-ano-20170514-0001.html

NAKASHIMA, Ellen (2015). **«New agency to sniff out threats in cyberspace»**. 2017, del portal The Washington Post. Sitio web: https://www.washingtonpost.com/world/national-security/white-house-to-create-national-center-to-counter-cyberspace-intrusions/2015/02/09/a312201e-afd0-11e4-827f-93f454140e2b_story.html?utm_term=.7eeb938533ce&wprss=rss_national

NICOLAS_POPP (2010). **«Google Hacked or Why the Cyber World Could Get M.A.D**»**. 2017, de Symantec Official Blog. Sitio web: https://www.symantec.com/connect/blogs/google-hacked-or-why-cyber-world-could-get-mad

NORTH ATLANTIC TREATY ORGANIZATION. **«Defence Against Terrorism Programme of Work (DAT POW)»**. 2017, de NATO. Sitio web: https://www.nato.int/cps/en/natohq/topics_50313.htm

NORTH ATLANTIC TREATY ORGANIZATION. **«Cyber defence»**. 2017, de NATO. Sitio web: https://www.nato.int/cps/en/natohq/topics_78170.htm

NORTH ATLANTIC TREATY ORGANIZATION. **«Countering terrorism»**. 2017, de NATO. Sitio web: https://www.nato.int/cps/en/natohq/topics_77646.htm

NOTICIA Y POLÍTICA. **Canal de TeleSUR TV**. 28 de mayo de 2014. **«Gobierno de Australia investiga ciberataques de hackers chinos»**. Reportaje perteneciente al programa televisivo "*Conexión Global*". Recuperado de: https://www.youtube.com/watch?v=1Fsp9RhYPhs

NUÑEZ VILLAVEIRÁN, Luis (2017). **«Hacktivistas: la amenaza del ciberespacio»**. De PAPEL, sección *Historias*. Portal web del diario El Mundo. Sitio web: http://www.elmundo.es/papel/historias/2017/08/22/599ac51e468aeba4728b4570.html

OPERACIÓN CONTRA EL CIBERTERRORISMO (2012). «Terroristas Informáticos 'Antifascistas' publican datos de clientes de comercios sevillanos para ser objetivos de sus acciones». Recuperado de: http://terroristasnogracias.blogspot.com/2012/02/operacion-contra-el-cibercrimen.html

ORGANIZACIÓN DE LAS NACIONES UNIDAS. **«Consejo de Seguridad: Comité contra el terrorismo»**. 2017. Sitio web: http://www.un.org/es/sc/ctc/

ORGANIZACIÓN DE LAS NACIONES UNIDAS PARA LA EDUCACIÓN, LA CIENCIA Y LA CULTURA. **«Definición de Gobernanza en Internet»**. 2017. Sitio web: http://es.unesco.org/themes/gobernanza-internet

OXFORD DICTIONARIES. Sitio web: https://www.oxforddictionaries.com/

PAGANINI, Pierluigi (2015). **«Spearphishing: A New Weapon in Cyber Terrorism»**. 2017, de Infosec Institute. Sitio web: http://resources.infosecinstitute.com/spearphishing-a-new-weapon-in-cyber-terrorism/#gref

PIGHI BEL, Pierina (2017). **«Qué es el Movadef, la polémica organización que vinculan con Sendero Luminoso en Perú y a la que acusan de apología al terrorismo»**. Del portal digital BBC Mundo. Sitio web: http://www.bbc.com/mundo/noticias-america-latina-40856626

QUARTZ STAFF (2015). **«'Call of Jihad': ISIS Turns to Video Games, Hollywood to Reach Recruits»**. 2017, del portal Defense One. Sitio web: http://www.defenseone.com/threats/2015/12/call-jihad-isis-turns-video-games-hollywood-reach-recruits/124709/

RAMADAN, Ahmad (2015). **«After the internet, TV is next on ISIS blacklist»**. 2017, del portal The Arab Weekly. Sitio web: http://www.thearabweekly.com/?id=1634

REDACCIÓN ÁMBITO (2010). **«Irán confirmó caso de ciberterrorismo»**. 2017, del portal Ámbito Financiero, sección *Tecnología*. Sitio web: http://www.ambito.com/544853-iran-confirmo-caso-de-ciberterrorismo

REDACCIÓN CAPITAL (2013) **«Anonymous Perú hackea web de entidades estatales»**. Del portal digital Radio Capital. Sitio web: http://www.capital.com.pe/2013-07-28-anonymous-peru-hackea-web-de-entidades-estatales-noticia_617378.html

REDACCIÓN CARACOL RADIO (2010). **«Gobierno anuncia mano dura contra el terrorismo informático»**. 2017, del portal Caracol Radio, sección *Judicial*. Sitio web: http://caracol.com.co/radio/2010/10/10/judicial/1286730420_369451.html

REDACCIÓN CIBERDERECHO (2014). **«Ciberterrorismo y sistemas críticos: Rusia vs Ucrania»**. 2017, del portal Ciberderecho. Sitio web: http://www.ciberderecho.com/ciberterrorismo-y-sistemas-criticos-rusia-vs-ucrania/

REDACCIÓN EC (2011). **«Anonymous atacó varios sitios web del Estado Peruano»**. Del portal El Comercio, sección *Tecnología*. Sitio web: http://elcomercio.pe/tecnologia/1284976/noticia-anonymous-ataco-hoy-varios-sitios-web-estado-peruano

REDACCIÓN EC (2017). **«Ciberseguridad mueve US$100 millones en el Perú»**. Del portal El Comercio, sección *Negocios*. Sitio web: https://elcomercio.pe/economia/negocios/ciberseguridad-mueve-us-100-millones-peru-noticia-446968

REDACCIÓN EC (2017). **«China efectuará una ley contra el ciberterrorismo y piratería desde el jueves»**. Del portal El Comercio, sección *Tecnología*. Sitio web: https://elcomercio.pe/tecnologia/tecnologia/china-efectuara-ley-ciberterrorismo-pirateria-jueves-426836

REDACCIÓN EFE (2008). **«La OTAN ultima el ingreso de tres países balcánicos, con dudas sobre Ucrania y Georgia»**. 2017, del portal El País. Sitio web: https://elpais.com/internacional/2008/03/06/actualidad/1204758011_850215.html

REDACCIÓN EFE (2015) **«Eugene Kaspersky: "El ciberterrorismo sólo requiere de gente que lo haga"»**. Del portal digital Diario Turing. Sitio web: http://www.eldiario.es/turing/Eugene-Kaspersky-amenaza-ciberterrorista-voluntades_0_358015047.html

REDACCIÓN EFE.; MELILLA/ LOGROÑO (2015). **«El 80% del adoctrinamiento yihadista se produce por internet»**. 2017, de El Heraldo, sección *Terrorismo*. Sitio web: http://www.heraldo.es/noticias/nacional/2015/07/23/el_del_adoctrinamiento_yihadista_produce_internet_403374_305.html

REDACCIÓN EFE (2016). **«Interpol exige más cooperación mundial contra el cibercrimen»**. 2017, de Eldiario.es, sección *Política*. Sitio web: http://www.eldiario.es/politica/Interpol-exige-cooperacion-mundial-cibercrimen_0_517249037.html

REDACCIÓN EL CONFIDENCIAL DIGITAL (2016). **«Israel enseña a España a luchar contra los *hackers* del Estado Islámico»**. Del portal El Confidencial Digital, sección *Defensa*. Sitio web: https://www.elconfidencialdigital.com/defensa/Israel-ensena-Espana-hackers-Islamico_0_2648735106.html

REDACCIÓN EL ESPECTADOR (2009). **«Policía investiga nuevo caso de terrorismo informático»**. 2017, del portal El Espectador, sección *Judicial*. Sitio web: https://www.elespectador.com/articulo167864-policia-investiga-nuevo-caso-de-terrorismo-informatico

REDACCIÓN EL ESPECTADOR (2010). **«Gobierno de Colombia busca penalizar el Ciberterrorismo»**. 2017, del portal El Espectador, sección *Nacional*. Sitio web: https://www.elespectador.com/noticias/nacional/articulo-228922-gobierno-buscara-penalizar-ciberterrorismo

REDACCIÓN EL PAÍS (2009). **«Corea del Sur y EE. UU., golpeados por el ciberterrorismo»**. 2017, del portal El País, sección *Tecnología*. Sitio web: https://elpais.com/tecnologia/2009/07/08/actualidad/1247041680_850215.html

REDACCIÓN EL PAÍS (2017). **«Vulnerabilidad informática: ciberataque afectó a 99 países»**. Del portal El País (UY). Sitio web: https://www.elpais.com.uy/mundo/vulnerabilidad-informatica-ciberataque-afecto-paises.html

REDACCIÓN EURONEWS (2015). **«La CIA anuncia una reorganización para combatir el ciberterrorismo»**. 2017, del portal Euronews. Sitio web: http://es.euronews.com/2015/03/07/la-cia-anuncia-una-reorganizacion-para-combatir-el-ciberterrorismo

REDACCIÓN EUROPA PRESS (2010). **«La cumbre de la OTAN se centra en la economía, el clima y el ciberterrorismo»**. 2017, del portal Europa Press, sección *Internacional*. Sitio web: http://www.europapress.es/internacional/noticia-cumbre-otan-centra-economia-clima-ciberterrorismo-20101120085259.html

REDACCIÓN GESTIÓN (2013). **«El Gobierno promulgó cuestionada ley de delitos informáticos»**. 2017, del portal Gestión, sección *Tecnología*. Sitio web: https://gestion.pe/peru/politica/gobierno-promulgo-cuestionada-ley-delitos-informaticos-51036

REDACCIÓN GESTIÓN (2017). **«Perú registrará US$ 4,782 millones en pérdidas por ciberdelitos en 2017»**. Del portal Gestión, sección *Tecnología*. Sitio web: https://gestion.pe/tecnologia/peru-registrara-us-4-782-millones-perdidas-ciberdelitos-2017-141411

REDACCIÓN HOMELAND SECURITY NEWS WIRE (2010). **«FBI: Cyber-terrorism a real and growing threat to U.S.»**. 2017, del portal Homeland Security News Wire, sección *Cibersecurity*. Sitio web: http://www.homelandsecuritynewswire.com/fbi-cyber-terrorism-real-and-growing-threat-us

REDACCIÓN IMAGINE TRENDS (2012). **«¿Hacia dónde camina nuestro miedo en la red? Del hacker al Ciberterrorismo»**. 2017, de Imagine Trends. Sitio web: https://imaginetrends.wordpress.com/2010/11/03/hacia-donde-caminan-los-virusvirus-informaticosciberterrorismohackersataques-informaticos-a-infraestructurasseguridad-en-la-redmiedo-en-la-redmiedo-a-ataques-internetamezazaciber/

REDACCIÓN INFOBAE (2014). **«Video: así decapitó el ISIS al periodista estadounidense Steven Sotloff»**. Del portal Infobae, sección *Política*. Sitio web: https://www.infobae.com/2014/09/02/1592006-video-asi-decapito-el-isis-al-periodista-estadounidense-steven-sotloff/

REDACCIÓN INFOBAE (2014). **«El Estado Islámico se radicaliza y difunde en video su ejecución más salvaje»**. Del portal Infobae, sección *Política*. Sitio web: https://www.infobae.com/2014/11/17/1609281-el-estado-islamico-se-radicaliza-y-difunde-video-su-ejecucion-mas-salvaje/

REDACCIÓN INFOBAE (2017). **«El Estado Islámico publicó dos videos: en uno utiliza a un niño para amenazar a Trump y en otro promete más ataques a España»**. Del portal Infobae, sección *Mundo*. Sitio web: https://www.infobae.com/america/mundo/2017/08/23/el-estado-islamico-publico-dos-videos-en-uno-utiliza-a-un-nino-para-amenazar-a-trump-y-en-otro-promete-mas-ataques-a-espana/

REDACCIÓN LA GACETA (2012). **«Allanan la casa de un tucumano investigado por "Ciberterrorismo" contra el Ejército de Colombia»**. 2017, de LA GACETA, sección *Policiales*. Sitio web: http://www.lagaceta.com.ar/nota/478615/allanan-casa-tucumano-investigado-ciberterrorismo-contra-ejercito-colombia.html

REDACCIÓN LA PRENSA (2013). **«En el Perú se pierden S/.98 millones cada año por delitos informáticos»**. Del portal La Prensa, sección *Actualidad*. Sitio web: https://laprensa.peru.com/actualidad/noticia-peru-se-pierden-s98-millones-cada-ano-delitos-informaticos-10217

REDACCIÓN LR (2013). **«Anonymous atacó webs de Perú y otros países de América»**. Del portal La República, sección *Sociedad*. Sitio web: http://larepublica.pe/sociedad/738359-anonymous-ataco-webs-de-peru-y-otros-paises-de-america

REDACCIÓN MERCADO (2010). **«Otra vez se relanza la OTAN. Su meta: el ciberterrorismo»**. 2017, del portal Mercado, sección *Economía y Política*. Sitio web: http://www.mercado.com.ar/notas/367046

REDACCIÓN Perú21 (2011). **«Anonymous no sería autor del ataque»**. Del portal digital Peru21. Sitio web: http://peru21.pe/noticia/830377/piden-ayuda-al-fbi-ataque-informatico

REDACCIÓN Perú21 (2012). **«El 57% de expertos piensa que hay una carrera armamentista en Internet»**. Del portal digital Peru21. Sitio web: http://peru21.pe/2012/01/31/tecnologia/57-expertos-piensa-que-hay-carrera-armamentista-internet-2009865

REDACCIÓN Perú21 (2012). **«Anonymous filtra 1,000 documentos del Gobierno peruano»**. Del portal digital Peru21. Sitio web: http://peru21.pe/2012/02/07/actualidad/anonymous-filtra-mil-documentos-gobierno-peruano-2010892

REDACCIÓN Perú21 (2012). **«Hackean a la Cancillería»**. Del portal digital Peru21. Sitio web: http://peru21.pe/2012/02/08/impresa/hackean-cancilleria-2010931

REDACCIÓN Perú21 (2013). **«Anonymous hackea webs del Estado»**. Del portal digital Peru21. Sitio web: http://peru21.pe/impresa/anonymous-hackea-webs-estado-2142237

REDACCIÓN Perú21 (2013). **«Ejecutivo presenta proyecto de ley que castiga 'Ciberdelitos' y pornografía»**. Del portal digital Peru21. Sitio web: http://peru21.pe/actualidad/ejecutivo-presenta-proyecto-ley-que-castiga-ciberdelitos-y-pornografia-infantil-2143746

REDACCIÓN Perú21 (2013). **«Ayacucho: Senderistas derriban torres de alta tensión y colocan banderas»**. Del portal digital Peru21. Sitio web: http://peru21.pe/politica/ayacucho-senderistas-derriban-torres-alta-tension-y-colocan-banderas-2162178

REDACCIÓN PERU.COM (2012). **«Anonymous publica casi 200 correos de Policía Informática»**. Del portal digital Peru.com, sección *Actualidad-Nacionales*. Sitio web: http://peru.com/2012/03/04/actualidad/nacionales/anonymous-publica-casi-200-correos-policia-informatica-noticia-45207

REDACCIÓN PUBLIMETRO (2013). **«Ciberataques aumentan un 30%»**. Del portal Publimetro.com, sección *Actualidad*. Sitio web: http://publimetro.pe/actualidad/15202/noticia-ciberataques-aumentan-30

REDACCIÓN PUBLIMETRO (2013). **«Un millón de víctimas diarias por Ciberdelitos»**. Del portal Publimetro.com, sección *Actualidad*. Sitio web: http://publimetro.pe/actualidad/1577/noticia-millon-victimas-diarias-ciberdelitos

REDACCIÓN RPP (2013). **«La Libertad: Anonymous ´hackea´ a empresa de agua Sedalib»**. 2017, del portal RPP, sección *Actualidad*. Sitio web: http://www.rpp.com.pe/2013-07-08-la-libertad-anonymous-hackea-a-empresa-de-agua-sedalib-noticia_611239.html

REDACCIÓN RPP (2013). **«FBI dispuesta a desarrollar programa de cooperación con policía peruana»**. 2017, del portal RPP, sección *Actualidad*. Sitio web: http://www.rpp.com.pe/2013-01-09-fbi-dispuesta-a-desarrollar-programa-de-cooperacion-con-policia-peruana-noticia_556232.html

REDACCIÓN SCIDEVNET (2016). **«Cybercrime in Africa: Facts and figures»**. 2017, del portal SciDevNet, sección *ICTs*. Sitio web: https://www.scidev.net/sub-saharan-africa/icts/feature/cybercrime-africa-facts-figures.html

REDACCIÓN SEGURIDAD INFORMÁTICA (2012). **«Panamá: Buscan penalizar intrusiones ilegales en sitios de internet»**. 2017, de Seguridad Digital [Fuente: Sdpnoticias]. Sitio web: http://seguinfo.wordpress.com/2012/03/10/panama-buscan-penalizar-intrusiones-ilegales-en-sitios-de-internet

REDACCIÓN TELESUR (2015). **«Venezuela demanda a Dolar Today en EE. UU. por ciberterrorismo»**. 2017, del portal TeleSur, sección *Mundo*. Sitio web: https://www.telesurtv.net/news/Venezuela-demanda-a-Dolar-Today-en-EE.UU.-por-ciberterrorismo-20151024-0004.html

REDACCIÓN UNIVISIÓN (2014). **«ISIS difundió el video de la decapitación del estadounidense Peter Kassig»**. Del portal Univisión Noticias. Sitio web: http://www.univision.com/noticias/noticias-del-mundo/isis-difundio-el-video-de-la-decapitacion-del-estadounidense-peter-kassig

REDACCIÓN ZONA MOVILIDAD (2016). **«Ciberterrorismo: Ucrania sufre un corte de electricidad por malware»**. 2017, del portal Zona Movilidad, sección *Tecnología*. Sitio web: https://www.zonamovilidad.es/noticia/12223/noticias-tecnologia-/ciberterrorismo:-ucrania-sufre-un-corte-de-electricidad-por-malware.html

REUTERS (2016). **«Un informe señala a piratas informáticos como responsables de un apagón en Ucrania»**. 2017, del portal Europapress, sección *Internacional*. Sitio web: http://www.europapress.es/internacional/noticia-informe-senala-piratas-informaticos-responsables-apagon-ucrania-20160110072937.html

REYES PLATA, Alejandro (2011). **«Ethical Hacking»**. 2017, de UNAM-CERT. Sitio web: https://www.cert.org.mx/historico/documento/index.html-id=7#Types

ROCHINA, Paula (2016). **«Hacktivismo: ¿Qué hay detrás de este movimiento activista?»**. 2017, de la revista digital de INESEM (Business School), sección *Tecnología*. Sitio web: https://revistadigital.inesem.es/informatica-y-tics/hacktivismo/

ROZOFF, Rick (2014). **«El Pentágono se asocia con la OTAN para crear un sistema de guerra ciberespacial global»**. 2017, de La Red 21, sección *Mundo*. Sitio web: http://www.lr21.com.uy/mundo/1176459-el-pentagono-se-asocia-con-la-otan-para-crear-un-sistema-de-guerra-ciberespacial-global

RÜHLE, Michael (2000). **«La OTAN, diez años después: aprendiendo lecciones»**. 2017, de Revista de la OTAN edición digital. Sitio web: https://www.nato.int/docu/review/2011/11-september/10-years-sept-11/ES/index.htm

SAGAR (2015). **«Cyberterrorism in India with special emphasis on Ahmadabad»**. Del portal Vanguardia (MX), sección *Internacional*. Sitio web: https://www.vanguardia.com.mx/articulo/se-alian-tres-paises-de-europa-para-combatir-ciberterrorismo

SAGNELLI, M. (2017). **«Se alían tres países de Europa para combatir ciberterrorismo»**. 2017, del portal Lawyers club India. Sitio web: http://www.lawyersclubindia.com/articles/Cyberterrorism-in-India-With-special-emphasis-on-Ahmadabad--2059.asp

SAMUEL, Alexandra (2004). **«Hacktivism and the future of political participation: Overview»**. 2017, del portal Alexandra Samuel. Sitio web: http://www.alexandrasamuel.com/dissertation/index.html

SATELL, Greg (2013). **«How the NSA uses social network analysis to map terrorist Networks»**. De Digital Toronto. Sitio web: http://www.digitaltonto.com/2013/how-the-nsa-uses-social-network-analysis-to-map-terrorist-networks/

SCHAFFERMAN, Karin Tamar (2017). **«Cyber-Terrorism»**. Del portal The Israel Democracy Institute. Sitio web: https://en.idi.org.il/articles/17488

SCHROTT, Urban (2016). **«Critical infrastructure: It's time to make security a priority»**. 2017, de ESET Ireland Official Blog. Sitio web: https://blog.eset.ie/2016/05/25/critical-infrastructure-its-time-to-make-security-a-priority/

S.E. (2012). **«Interior e Industria firman un acuerdo contra el ciberterrorismo y el cibercrimen»**. Del portal ABC.es, sección Seguridad. Sitio web: http://www.abc.es/20121005/espana/abci-interior-industria-firman-acuerdo-201210042020.html

SEGALL, Laurie (2014). **«Las tácticas de reclutamiento de ISIS: redes sociales y videojuegos»**. 2017, del portal CNN. Sitio web: http://cnnespanol.cnn.com/2014/09/30/las-tacticas-de-reclutamiento-de-isis-redes-sociales-y-videojuegos/#0

STEPHEN, Katherine (2015) **«UAB research finds automated voice imitation can fool humans and machines»**. 2017, de UAB News - The University of Alabama at Birmingham. Sitio web: http://www.uab.edu/news/research/item/6532-uab-research-finds-automated-voice-imitation-can-fool-humans-and-machines

SOLON, Olivia (2017) **«The future of fake news: don't believe everything you read, see or hear»**. 2017, del portal web The Guardian, sección Tecnologías. Sitio web: https://www.theguardian.com/technology/2017/jul/26/fake-news-obama-video-trump-face2face-doctored-content

SUCASAS FERNÁNDEZ, Ángel Luis (2016). **«El cibercrimen, el negocio más rentable»**. Del portal digital EL PAÍS, sección *Ciberseguridad*. Sitio web: https://elpais.com/tecnologia/2016/03/16/actualidad/1458146832_730308.html

SUWAJANAKORN, Supasorn; SEITZ, Steven M. & KEMELMACHER-SHLIZERMAN, Ira (2017) **«Synthesizing Obama: Learning Lip Sync from Audio SIGGRAPH 2017»**. 2017, de GRAIL: Graphics and Imaging Laboratory of the University of Washington's. Sitio web: http://grail.cs.washington.edu/projects/AudioToObama/

SYMANTEC PRESS CENTRE (2002). **«Symantec CEO Raises Awareness of Cyber Terrorism»**. 2017, de Symantec. Sitio web: http://www.symantec.com/region/au_nz/press/au_021107.html

THEILER, Olaf (2000). **«Nuevas amenazas: el ciberespacio»**. 2017, de Revista de la OTAN edición digital. Sitio web: https://www.nato.int/docu/review/2011/11-september/Cyber-Threads/ES/index.htm

TREND MICRO (2014). **«Cyber attacks considered top national security threat»**. 2017, de Trend Micro Blog. Sitio web: https://blog.trendmicro.com/cyber-attacks-considered-top-national-security-threat/

TREND MICRO (2015). **«The two sides of encryption: Protection for and against cybercrime»**. 2017, de Trend Micro Blog. Sitio web: https://blog.trendmicro.com/the-two-sides-of-encryption-protection-for-and-against-cybercrime/

VALERA, Ramón (2015). **«Forbes admite un error en su artículo sobre el uso de PS4 por los terroristas de París»**. 2017, del portal Vandal, sección Noticias. Sitio web: http://www.vandal.net/noticia/1350670713/forbes-admite-un-error-en-su-articulo-sobre-el-uso-de-ps4-por-los-terroristas-de-paris/

VILLAMIL, Eduardo (2017). **«Los videojuegos: un elemento más de la propaganda terrorista»**. Del portal El Imparcial. Sitio web: https://www.elimparcial.es/noticia/180729/sociedad/los-videojuegos:-un-elemento-mas-de-la-propaganda-terrorista.html

WAGNER, Daniel (2017). **«Why New Laws Won't Stop Cyber Terrorism»**. Del portal Huffpost (US Edition). Sitio web: https://www.huffingtonpost.com/entry/why-new-laws-wont-stop-cyber-terrorism_us_5937d009e4b04ff0c46682f8

WIKILEAKS. **«About WikiLeaks»**. 2017, de WikiLeaks. Sitio web: http://wikileaks.org/

YIN-POOLE, Wesley (2015). **«Sony responds to claim PS4 used for terrorist communications»**. 2017, del portal Eurogamer. Sitio web: http://www.eurogamer.net/articles/2015-11-16-sony-responds-to-claim-ps4-used-for-terrorist-communications

ZAISER, Ariel (2014). **«Tras el conflicto Rusia-Ucrania, el vacío jurídico del ciberterrorismo»**. 2017, del portal Equilibrium Global, sección *Geopolítica*. Sitio web: http://equilibriumglobal.com/tras-el-conflicto-rusia-ucrania-el-vacio-juridico-del-ciberterrorismo/

ZAZO GUIJARRO, Lara (2013). **«Periodistas, en el punto de mira de los ciberterroristas»**. Del portal ComputerHoy.com, sección *Noticias*, subsección Apps. Sitio web: http://computerhoy.com/noticias/apps/periodistas-punto-mira-ciberterroristas-3099

ZWIENENBERG, Righard (2016). **«From Georgia With Love: Win32/Georbot information stealing trojan and botnet»**. 2017, del portal We Live Security, categoria *Viruses Revealed*. Sitio web: https://www.welivesecurity.com/2012/03/21/win32georbot-information-stealing-trojan-botnet-from-georgia-with-love/

ANEXOS

Anexo N°01 Matriz de consistencias

PROBLEMA	OBJETIVOS	HIPÓTESIS	VARIABLE	METODOLOGÍA
Problema General	***Objetivo General***	***Hipótesis General***	***Variable I***	***Método Inductivo***
¿Debe considerarse a la figura del ciberterrorismo como una figura delictiva en el Perú?	Establecer la necesidad de que en nuestro país se tipifique como delito la figura del ciberterrorismo.	La figura del ciberterrorismo constituye alta peligrosidad para nuestra nación, especialmente porque este no ha sido considerado como un delito en nuestra legislación.	La figura del ciberterrorismo como delito reconocido en nuestro país.	Parte de información recogida mediante sucesiva observación para establecer ley mediante generalización. Se basa en verdades particulares para llegar a verdad universal.
Problemas Específicos	***Objetivos Específicos***	***Hipótesis Específicas***	***Variable II***	***Método de Análisis***
• Qué tipo de figura delictiva sería la figura del ciberterrorismo: ¿Delito contra el Estado o simplemente un ciberdelito? • ¿El Perú cuenta con tecnología suficiente para poder combatir o resistir un ciberataque derivado de la figura del ciberterrorismo?	• Analizar el tipo de figura delictiva que corresponde la figura del ciberterrorismo. • Determinar si el país cuenta con la tecnología y elementos legales suficientes para combatir o resistir un ciberataque a causa de la figura del ciberterrorismo.	• El desarrollo de las TIC otorga elementos que facilitan la expansión de la figura del ciberterrorismo en nuestra nación. • La falta de una legislación que tipifique la figura del ciberterrorismo genera un vacío legal aprovechado por los cibercriminales para ejecutar acciones terroristas en Internet.	La figura del ciberterrorismo constituye alta peligrosidad para nuestra nación gracias al uso de Internet y TIC.	Operación intelectual que consiste en considerar por separado las partes de un todo.

Anexo N°02 Glosario de términos

A

Abandonware Programas descatalogados que mantienen su estado legal, haciendo que su descarga, por más que la empresa creadora desaparezca o quiebre, siga siendo ilegal. Su existencia se produce mayormente en el campo de los videojuegos. Este es un término que no es reconocido en el ámbito legal y no puede usarse en el campo de los derechos de autor.

B

Botnet Proveniente de los términos *robot* y *network*, es un virus troyano utilizado para vulnerar la seguridad de las computadoras de varios usuarios para tomar el control y organizarlas en una red *bot* que pueden administrarse de manera remota para realizar ataques que el delincuente decida, como ataques spam o DDoS a gran escala.

C

Centennial Generación compuesta por personas nacidas desde el año 1997 en adelante y que ha conocido la vida con el empleo de las tecnologías desde su nacimiento, influyendo en sus hábitos y comportamientos. También llamada Generación Y.

CERT Computer Emergency Response Team (Equipo de Respuesta ante Emergencias Informáticas).

CERT/CC CERT Coordination Center.

Cibercriminal **I**ndividuo que se aprovecha de las vulnerabilidades de las redes y sistemas de información para llevar a cabo actos tipificados por ley como criminales: robo de información, destrucción información, extorsión, divulgación de información confidencial, distribución de pornografía infantil, envío de correo basura, terrorismo, fraudes, robo de identidad, falsificación de información, piratería, etc.

CICTE Comité Interamericano contra el terrorismo.

CIDH Corte Interamericana de Derechos Humanos.

CNDH Comisión Nacional de Derecho Humanos (MX).

CONASEC Sistema Nacional de Seguridad Ciudadana (Perú).

CONSTITUENCY Comunidad de la que el CERT/CSIRT es responsable y a la que ofrece sus servicios.

Cracker Persona que entra en un sistema informático sin autorización, cuyo propósito es hacer daño (destruir archivos, robar números de tarjetas de crédito, virus de plantas, etc.). También llamados especialistas en inseguridad cibernética o ingenieros en inseguridad cibernética.

Cracking Obtener acceso no autorizado a los sistemas informáticos para cometer un delito, como cavar en el código para hacer un programa protegido contra copia e inundar sitios de Internet, negando así el servicio a los usuarios legítimos.

CSIRT Computer Security Incident Response Team (Equipo de Respuesta ante Incidencias de Seguridad).

CTITF Counter-Terrorism Implementation Task Office.

CTO Chief Technical Officer (Director Técnico).

Cybercrook Persona que comete actividades criminales por medio de computadoras o de Internet. Un cibercriminal.

D

Dark web Internet oscura. Parte de la Deep web que solo constituye el 0.1% de Internet.

DDoS Ataque de denegación de servicio.

Deep web Internet profunda. En esta se encuentra contenido que no ha sido indexado a los buscadores convencionales. Constituye el 90% de Internet.

E

ENISE Encuentro Internacional de Seguridad de la Información.

Ethical Hacking Hackeo ético. Actividad en donde se vulneran sistemas valiéndose de test de intrusión para valorar su seguridad física y lógica.

Exploit Un programa o sistema diseñado para aprovechar un error particular o vulnerabilidad de seguridad en equipos o redes. Un programa de software aprovechando vulnerabilidades en software.

F

Fake news Noticias falsas.

G

Gamer Jugador de videojuegos.

H

Hack Código fuente de un programa.

Hacker Persona que disfruta de aprender los detalles del sistema informático y cómo sacar provecho de sus capacidades. También llamados especialistas en ciberseguridad o ingenieros en ciberseguridad.

Hacking Acto de sumergirse en los detalles de los sistemas informáticos para optimizar sus capacidades.

Hacktivismo Hacer hacking, phreaking o crear tecnología para conseguir un objetivo con fines reivindicativos de derechos, promulgación de ideas políticas o quejas de la sociedad en general.

Hardware Conjunto de elementos físicos o materiales que constituyen una computadora o un sistema informático.

I

ICANN Corporación de Internet para la Asignación de Nombres y Números.

IMP Procesadores de mensajes de interfaz.

INCIBE Instituto Nacional de Ciberseguridad.

INEI Instituto Nacional de Estadística e Informática (Perú).

INTERNET Red informática mundial, descentralizada, formada por la conexión directa entre computadoras mediante un protocolo especial de comunicación conocido como protocolos TCP/IP.

INTERPOL International Criminal Police Organization.

ISOC Internet Society.

ISRT Internet Security Threat Report.

M

M^{3}AAWG The Messaging, Malware and Mobile Anti-Abuse Working Group.

Malware Software malicioso que interfiere con las funciones normales del ordenador o envía datos personales sobre el usuario a partes no autorizadas a través de Internet o realiza otras funciones maliciosas.

Millenial Generación compuesta por personas nacidas entre los años 1980 y 1995 y que ha conocido la vida con el crecimiento y desarrollo de la tecnología. También llamada Generación Z.

MOD Extensión del software que modifica y brinda nuevas características a un videojuego original, como nuevos niveles, personajes, jugabilidad, entre otros.

Multistakeholder Modelo de múltiples partes interesadas.

N

NSF National Science Foundation.

O

OAS Organization of American States.

OCDE Organización para la Cooperación Económica y el Desarrollo.

OEA Organización de Estados Americanos.

ONG Organización No Gubernamental.

ONU Organización de las Naciones Unidas.

OTAN Organización del Tratado del Atlántico Norte.

P

PeCERT Coordinadora de Respuestas a Emergencias en Redes Teleinformáticas de la Administración Pública del Perú.

Penetration Testing Prueba de penetración o *pentest*. Ejercicio utilizado en el ethical hacking contra los mecanismos de defensa con el propósito de encontrar debilidades en la seguridad, funcionalidad y datos, sea en dispositivos físicos, digitales y factor humano.

Phishing Modalidad a través de la cual se busca obtener información de manera fraudulenta, ya sea por medio de ingeniería social o mensajería.

Phreaker Persona que investiga y practica el arte de pasearse por las redes telefónicas, por ejemplo, para hacer llamadas internacionales gratuitas sin importar la central telefónica y a nivel internacional.

Phreaking Interceptar una línea telefónica para hacer llamadas de larga distancia o insertar comentarios incómodos.

R

Ransomware Programa que restringe el acceso a su sistema y exige el pago de un rescate para eliminar la restricción.

S

Software Programas y rutinas para una computadora o el material del programa para un dispositivo electrónico que lo hace funcionar.

Spearphishing Estafa que se ejecuta por medio de correo electrónico o comunicaciones dirigidas a un blanco específico, sea empresa, organización o persona, con el propósito de robar información o instalar un malware en el sistema.

Spyware Software que recopila información personal sobre los usuarios y sus actividades sin su conocimiento o consentimiento.

T

TELECOM Telecomunicaciones.

Terrorismo Uso sistemático del terror1 para coaccionar a sociedades o gobiernos, utilizado por una amplia gama de organizaciones, grupos o individuos en la promoción de sus objetivos, tanto por partidos políticos nacionalistas y no nacionalistas, de derecha como de izquierda, así como también por corporaciones, grupos religiosos, racistas, colonialistas, independentistas, revolucionarios, conservadores y gobiernos en el poder.

TIC Tecnologías de la información y comunicación.

Torrent Fichero que permite abrir y descargar archivos utilizando el protocolo P2P (red entre iguales). Utilizado para el acceso a la Deep web.

U

UNODC United Nations Office on Drugs and Crime.

V

Videojuego Software interactivo que se utiliza para entretenimiento, juegos de rol y simulación, que puede ser jugado en un dispositivo especializado (consola de videojuegos), dispositivo móvil, computadora, entre otros.

Virus Tipo de malware intrusivo que se replica e inserta copias de sí mismo en programas legítimos, donde realiza operaciones no deseadas ya menudo dañinas, y que afecta el funcionamiento del dispositivo infectado, destruyendo total o parcialmente la información almacenada.

W

Worm Un tipo de malware que se replica a través de una red de ordenadores haciendo copias de sí mismo, que envía a otras computadoras. Un gusano se incrusta en la memoria y puede replicarse tantas veces que causa que el host se bloquee.

WWW World Wide Web.