ANÁLISIS DE LA INFLUENCIA DEL FENÓMENO DEL CIBERTERRORISMO EN LAS DINÁMICAS DE SEGURIDAD DE LA UNIÓN EUROPEA

JULIÁN ALEJANDRO TORRES PEDRAZA

UNIVERSIDAD COLEGIO MAYOR DE NUESTRA SEÑORA DEL ROSARIO
FACULTAD DE RELACIONES INTERNACIONALES
BOGOTÁ D.C., 2014

“Análisis de la influencia del fenómeno del Ciberterrorismo en las dinámicas de seguridad de la Unión Europea”

Proyecto de Monografía de grado
Presentada para optar por el título de
Internacionalista
En la Facultad de Relaciones Internacionales
Universidad Colegio Mayor de Nuestra Señora del Rosario

Presentado por:
Julián Alejandro Torres Pedraza

Dirigida por:
Andrés Gaitán Rodríguez

Semestre I, 2014

RESUMEN

El fenómeno del ciberterrorismo se constituye como una nueva amenaza a la seguridad internacional, este fenómeno es el resultado de distintos procesos en el sistema internacional como el de la globalización. La definición del concepto se establece por la convergencia entre el ciberespacio y el terrorismo. El objetivo de esta investigación es explicar las distintas dimensiones del ciberterrorismo, métodos de ataque, acciones pasadas, propósito del fenómeno, situación actual y vulnerabilidades. El objeto de estudio de esta investigación es la Unión Europea como actor del sistema internacional que se ha visto afectado por este fenómeno. También se dará uso al aparato teórico de los complejos de seguridad desarrollado por Barry Buzan para evidenciar las nuevas amenazas del sistema internacional y analizar los procesos de securitización del fenómeno en el seno de la Unión Europea.

Palabras Clave:

Ciberespacio, Infraestructuras críticas, Métodos de Ataque, Ciberterrorista, Complejo de seguridad, Internet, Ciberataques.

ABSTRACT

Cyberterrorism is a new threat for the international security; this phenomenon is the result of different processes in the international system as the globalization, the definition of the concept should be focus in the merge of the cyberspace and the terrorism. This research would provide a clear explanation of the cyberterrorism methods, past actions, means of penetration, current situation and vulnerabilities. The analysis of this threat takes place in the European Union as an actor that has suffered the consequences of cyberterrorism. In the same time the investigation uses the theory of the Regional Security Complex of Barry Buzan with the purpose of explaining the new security threats and the challenges of the European Union to set clear measures to diminish the impact of cyberterrorism.

Key Words:

Cyberspace, Critical Infrastructure, Methods of attack, Cyber terrorist, Security complex, Internet, Cyber attacks.

A Dios, por sus bendiciones.

A mis padres, por su amor incondicional y ejemplo de vida.

A mis hermanos, por su compañía y lealtad.

AGRADECIMIENTOS

Doy gracias a Dios por todas las bendiciones recibidas. A mis padres por ser el ejemplo de esfuerzo, dedicación, constancia, sabiduría y amor. Gracias por compartir y ser participes de mis sueños y metas, espero que puedan acompañarme en mi desarrollo como profesional y ser humano. Todo lo que he logrado es gracias a su sacrificio, los amo eternamente. A mis hermanos por su compañía, consejos, complicidad y guía. Me siento muy orgulloso de cada uno de ustedes y sé que la vida y Dios los premiará. A mi tía Gloria por compartir mis alegrías y tristezas.

Doy gracias a mi director de monografía Andrés Gaitán, por su disposición, consejos, recomendaciones y paciencia. Gracias por ayudarme a culminar esta etapa profesional. Quiero hacer extensiva mi gratitud a todas las personas de la Universidad del Rosario que intervinieron en mi formación profesional y personal.

CONTENIDO

		Pág.
INTRODUCCIÓN		9
1.	TEORÍA DE LOS COMPLEJOS DE SEGURIDAD REGIONAL: UNIÓN EUROPEA	12
1.1.	Evolución de la Teoría de los Complejos de Seguridad Regional	13
1.2.	Securitización	16
1.3.	Niveles de análisis, variables y posibles evoluciones de un Complejo de Seguridad	19
1.4.	Tipos de Complejos de Seguridad	21
2.	CIBERTERRORISMO: FORMACIÓN, PARADIGMAS Y CAPACIDADES DE LA NUEVA AMENAZA	24
2.1.	Guerra en red	25
2.2.	Ciberterrorismo	29
2.3	Tácticas del Ciberterrorismo	33
2.4	Actos Ciberterroristas y posibles escenarios futuros	40
3.	ACTUACIÓN DE LA UNIÓN EUROPEA EN CONTRA DEL FENÓMENO DEL CIBERTERRORISMO	44
3.1.	Instituciones de la UE encargadas de la ciberseguridad	44
3.2.	Respuesta de la Unión Europea	46

3.3. Respuesta de los Estados Miembros 51

3.4. La Unión Europea en busca del establecimiento de una política concreta contra el Ciberterrorismo: “Clean It Project” 52

4. CONCLUSIONES 55

BIBLIOGRAFÍA

LISTA DE ANEXOS

Anexo 1. Tabla: Secretaria de Estado de los Estados Unidos de América. “Sitios Web de Organizaciones Terroristas 2002”.

Anexo 2. Documento: Unión Europea. “Estrategia de Seguridad Interior de la Unión Europea “Hacia un modelo europeo de seguridad 2010-2014”

Anexo 3. Documento: “Estrategia de Ciberseguridad de la Unión Europea del 2013”

INTRODUCCIÓN

Actualmente el sistema internacional se encuentra inmerso en las dinámicas del desarrollo tecnológico, las comunicaciones y sistemas informáticos, estas determinan la consolidación de redes interdependientes, participación de nuevos actores y nuevos procesos en la configuración de poder. El desarrollo de internet como mecanismo de comunicación, difusión y elaboración de información ha traído consigo nuevos retos en materia de seguridad. Las actividades cibernéticas han vulnerado la capacidad de respuesta de los Estados en esta área. Dada la evolución de las relaciones internacionales y los procesos emanados de la globalización y desarrollo cibernético se han generado nuevas amenazas como el ciberterrorismo, temática que se posiciona en la agenda de seguridad internacional.

La tesis de esta monografía es analizar la influencia del fenómeno del Ciberterrorismo en la Unión Europea y determinar mediante el uso de un aparato teórico las consecuencias de dicho fenómeno en las dinámicas de seguridad de la UE. Igualmente, se busca evidenciar el impacto de un fenómeno actual como el Ciberterrorismo en materia de seguridad, que atenta contra la estabilidad de los Estados y la sociedad.

El alcance de esta investigación contiene un componente descriptivo y explicativo. Para el desarrollo de esta monografía resulta indispensable describir el ciberterrorismo como amenaza a la seguridad internacional en todas sus dimensiones, partiendo de la construcción e identificación del fenómeno, mecanismos y estrategias que se desarrollan en el accionar de dicho fenómeno. En concreto se busca describir los componentes y características del ciberterrorismo con el propósito de brindar al lector la posibilidad de identificar las consecuencias que se emanan de esta nueva amenaza a la seguridad internacional. El componente explicativo de la investigación se sustenta en la necesidad de explicar cómo el fenómeno del ciberterrorismo ha influenciado las dinámicas de seguridad de la Unión Europea, explicar los alcances de esta amenaza en la consolidación de políticas, estrategias y programas que buscan proteger los sistemas de información e infraestructuras críticas de la UE y sus Estados miembros.

Para el desarrollo de la investigación y comprobación de hipótesis se requiere de la aplicación de una teoría que permita dar respuesta y análisis al fenómeno que se describe. En esta investigación se aplicará la teoría de los complejos de seguridad regional elaborada por Barry Buzan, dicha teoría permite evidenciar el impacto y proceso de securitización de las nuevas amenazas. También nos permite evidenciar el proceso que se ha generado al interior de la UE y en la seguridad nacional de los Estados miembros. La teoría escogida trae consigo un marco conceptual que garantiza la aplicación relacional del fenómeno con el objeto de estudio. La descripción teórica y su aplicación en las dinámicas de seguridad en la Unión Europea serán explicadas en el primer capítulo.

El segundo capítulo describe el fenómeno del ciberterrtorismo como amenaza a la seguridad internacional en todas sus dimensiones, su historia, proceso de consolidación, características, evolución y proyección como amenaza para evidenciar los desafíos que se presentan en materia de seguridad. Finalmente, el tercer capítulo busca explicar la aplicación relacional del fenómeno del ciberterrorismo con el objeto de estudio (Unión Europea), analizar las estrategias, políticas y medidas que se han aplicado en el ámbito local y regional.

El carácter de esta investigación es longitudinal no experimental en la medida que se espera analizar la correlación entre el fenómeno del ciberterrorismo (variable independiente) y la seguridad en la Unión Europea (variable dependiente). Se pretende explicar cómo la variable independiente ha influido en la reconfiguración de la variable dependiente sin alterar premeditadamente las variables. Dado el carácter longitudinal de la investigación se adopta un enfoque institucionalista para explicar la incidencia del fenómeno en las dinámicas de seguridad de la UE y en las instituciones internas que regulan y proporcionan los lineamientos de seguridad cibernética. Es así como el enfoque institucional proporciona una perspectiva de análisis correspondiente al objetivo de la investigación.

Esta monografía busca contribuir a la academia y a la sociedad, en la medida que dadas las características del fenómeno, todos somos vulnerables a ser víctimas del ciberterrorismo. Esta monografía va dirigida a distintos actores de la sociedad, tomadores

de decisión, estudiantes y usuarios de la red que hacen parte de lo que se denomina como ciberespacio.

El análisis e investigación de las nuevas temáticas de la agenda de seguridad internacional son indispensables para entender la creación de distintas estrategias de seguridad nacional e internacional, que determinan las relaciones de poder en el sistema internacional.

1. TEORÍA DE LOS COMPLEJOS DE SEGURIDAD REGIONAL: UNIÓN EUROPEA

Las nuevas características del sistema internacional son el resultado de distintos procesos históricos, culturales, económicos y sociales que determinan las relaciones entre los actores que configuran el sistema internacional. El ciberterrorismo se presenta como una nueva amenaza a las dinámicas de seguridad mundial, trayendo consigo retos en materia de seguridad y de establecimiento de estructuras que protejan la seguridad de los estados y demás actores del sistema internacional. Dicho fenómeno debe ser analizado como una consecuencia al surgimiento y desarrollo cibernético que se ha presentado en el marco de la globalización.

La influencia del fenómeno del ciberterrorismo en las dinámicas de seguridad de la Unión Europea requiere del estudio y aplicación de un marco teórico que dé cuenta de los procesos y mecanismos que se han generado al interior de la UE para hacer frente a dicho fenómeno. Es por esta razón que se ha determinado utilizar el aparato teórico que proporciona Barry Buzan con la Teoría de los complejos de seguridad regional como marco teórico principal en la investigación. Las perspectivas sobre las dinámicas de seguridad son diferentes y se abordan aspectos no relacionados en las teorías tradicionales. Barry Buzan es uno de los autores representantes de la Escuela de Copenhague y su teoría de los complejos de seguridad regional es un aporte contemporáneo y diverso al análisis de las nuevas nociones de seguridad.

El objetivo de este capítulo es proporcionar de una manera descriptiva los principales aportes de la Teoría de los Complejos de Seguridad Regional, su origen, variables, conceptos, niveles de análisis, definiciones y categorías que se establecen a la luz de este aparato teórico en relación con la Unión Europea como objeto de estudio. Cabe resaltar que este acápite presentará las bases teóricas para poder entender la actuación de la Unión Europea en contra del Ciberterrorismo y así mismo la descripción y aplicación de esta teoría en el marco de sus principales enunciados.

1.1. Evolución de la Teoría de los Complejos de Seguridad Regional

La Teoría de los Complejos de Seguridad Regional es el resultado teórico de explicación de la configuración y dinámicas de seguridad del sistema internacional de la postguerra fría. El periodo de la guerra fría se caracterizó por la existencia y predominio de las dos superpotencias, Estados Unidos y la Unión Soviética. Poderes que determinaban el modus operandi del Sistema Internacional, minimizando las dinámicas regionales en el análisis y actuación en materia de seguridad. Cabe resaltar que el entramado teórico de este periodo estaba determinado por la corriente realista de las relaciones internacionales, sustentado en el constante análisis de poder y supervivencia de los Estados bajo un enfoque político-militar.

En el transcurso de la bipolaridad los conflictos y dinámicas regionales estaban supeditados a las necesidades e intereses de las superpotencias. La internacionalización de los conflictos regionales se presentó como una suerte de campo de batalla entre las dos superpotencias, se dio uso a la inestabilidad de distintas regiones del mundo para poder enfrentar las capacidades y desarrollo militar de Estados Unidos y la Unión Soviética.

Con la desintegración de la Unión Soviética a principios de la década de los 90’s se recupera parcialmente la autonomía regional en materia de seguridad, los procesos y determinaciones en esta área estarían enmarcados en ámbitos locales y regionales, determinados por el grado de institucionalización e integración de los Estados. Dada la coyuntura en la configuración del sistema internacional distintos académicos entre ellos Barry Buzan desarrollaron aparatos teóricos sobre la nueva configuración de las relaciones de seguridad entre los Estados y las regiones. Igualmente se enmarcó la relevancia de ampliar la agenda de seguridad hacia un espectro mas comprehensivo, diferenciado del enfoque tradicional basado en términos netamente político-militares, enfoque que se restringe en el análisis de las dinámicas contemporáneas y multidimensionales de las relaciones internacionales.

El enfoque de la teoría de los complejos de seguridad regional de Buzan es el de la Escuela de Copenhague, centro de pensamiento que a lo largo de su evolución ha proporcionado distintos estudios y teorías comprehensivas del sistema internacional. Su enfoque de investigación se centra en los temas de seguridad internacional haciendo énfasis

en la ampliación de la noción de seguridad hacia un espectro económico, ambiental y social.

La teoría de los complejos de seguridad regional utiliza distintas contribuciones de enfoques teóricos como el neorrealismo, globalismo y constructivismo en materia del análisis de las relaciones internacionales y de seguridad, sin embargo esta teoría abarca las nuevas dinámicas presentes en el sistema internacional determinadas por la globalización.

El neorrealismo propuesto por Kenneth Waltz enuncia la importancia del nivel de análisis sistémico o global, adicionalmente esta corriente teórica identifica el estudio de seguridad a la luz del ámbito nacional y global. En complemento la teoría de los complejos de seguridad regional proporciona y da prioridad al nivel de análisis del subsistema, así mimo las dinámicas regionales se interpretan como una suerte de intermedio entre las interacciones globales y nacionales. Este internacionalistas afirma que este nuevo nivel de análisis permite hacer estudios prácticos en materia de seguridad, ya que la relaciones entres los Estados y unidades se encuentran suficientemente conectadas, lo cual genera la necesidad de entender las amenazas y acciones en materia de seguridad en conjunto y no como unidades.

A diferencia del neorrealismo Barry Buzan propende por el entendimiento y desarrollo del concepto de seguridad desde una perspectiva constructivista. "Este tratamiento se da en la medida en que los autores conciben la formación de estos complejos con base en patrones de amistad y enemistad, que hacen que los subsistemas regionales dependan de las acciones e interpretaciones de los actores, no solo que obedezcan a un cálculo de la distribución de poder" (Cujubante 2013, pág. 104). El proceso de securitización se determina por la capacidad y necesidad de dar respuesta a las amenazas de manera conjunta y no independientemente por las unidades, Las amenazas a la seguridad surgen de la percepción que se tiene al interior de un complejo.

Sumado a lo anteriormente expuesto la teoría de los complejos de seguridad regional aplica elementos del globalismo, en referencia a las implicaciones que trae el desarrollo tecnológico, las dinámicas comerciales, el avance de los medios de comunicación en la seguridad de los Estados y regiones. La globalización trae consigo distintos retos multidimensionales en materia de seguridad, que a su vez implican la

consolidación de modelos y estrategias conformes a la contemporaneidad de los fenómenos.

El profesor emérito en relaciones internacionales del London School of Economics presenta una primera definición de los complejos de seguridad regional en 1983 en el libro *People, States and Fear,* los complejos de seguridad se definen como un grupo de Estados cuyas preocupaciones de seguridad están lo suficientemente interrelacionadas que sus problemas de seguridad nacional no pueden ser considerados y analizados unos aparte de otros (Buzan 1991, pág. 106). Buzan enuncia la diversidad de factores que permiten la interrelación entre los Estados, factores geográficos, estratégicos, políticos, económicos, culturales e históricos determinan el establecimiento de los complejos de seguridad. En esta definición se puede esbozar el propósito teórico determinado por el análisis de las relaciones internacionales de seguridad desde un nivel de análisis regional. Los Estados perciben las amenazas de seguridad como un problema común, por ende las acciones y medidas para hacer frente a las amenazas surgen de la incapacidad individual de dar solución y respuesta.

Este analista de seguridad internacional explica el surgimiento de los complejos de seguridad como resultado de la estructura anárquica del Sistema Internacional, así mismo establece la utilidad de dicha teoría en el marco de los procesos de toma de decisión en los Estados y las regiones en términos de seguridad. Este aporte teórico involucra los aspectos macro y micro del sistema internacional. El macro nivel permite analizar la influencia que tienen las superpotencias en los procesos del sistema, y así mismo la respuesta que se da en términos locales frente a las dinámicas presentadas por el macro nivel. En contraste, en el análisis del micro nivel se pueden evidenciar las interacciones que se presentan a nivel local o nacional, y como se enfrentan las problemáticas que se introducen desde el macro nivel (Buzan 1983, págs. 111 – 112).

La definición de los complejos de seguridad regional sufrió una modificación en el libro *Regions and Powers de 1998*. Buzan junto con Ole Waever sustentan la necesidad de ampliar el espectro de análisis de los actores que forman parte de los complejos de seguridad, en respuesta a las dinámicas presentes en el sistema internacional caracterizadas por relaciones entre diversos actores estatales y no estatales. Es así como se amplía la

concepción Estatocéntrica hacia un conjunto de "unidades", sin embargo es importante recalcar que para los autores el Estado sigue siendo el principal actor en materia de seguridad y de las relaciones internacionales. Otro cambio que se introdujo fue la ampliación de la agenda de seguridad enmarcada en términos político-militares, hacia una agenda multisectorial. Estos cambios propendían dar un análisis más acertado de las dinámicas regionales en materia del análisis de seguridad y la actuación de las unidades en el marco de los complejos de seguridad[1].

1.2. Securitización

En la revisión que hace el autor sobre la definición de los complejos de seguridad regional se introduce el término de securitización. Este se refiere a la percepción de amenazas existenciales como el ciberterrorismo por parte de las unidades del complejo de seguridad. Dichas amenazas atentan directamente contra la seguridad nacional y supervivencia de la población, por lo cual es necesaria la implementación de medidas y acciones extraordinarias que den respuesta a la problemática que se plantea. Buzan afirma que este tipo de medidas extraordinarias pueden constituirse en detrimento de los marcos legales establecidos, sin embargo se justifican dada la amenaza existencial.

Es importante resaltar que durante el proceso de securitización la amenaza existencial puede ser objetiva o subjetiva. La amenaza se puede constituir en términos realistas o tangibles, o puede presentarse con base a una percepción que se tiene de la existencia y efectos de esta. "La exacta definición y criterio de securitización está constituida por el establecimiento intersubjetivo de una amenaza existencial con suficiente proyección como para tener efectos políticos sustanciales" (Buzan y Weaver 1998, pág.25). Como lo presenta el autor hay tres componentes que determinan el éxito de la securitización de un problema, la existencia de una amenaza existencial, la respuesta por medio de acciones y medidas de urgencia, y el análisis de las consecuencias que traen estas medidas en el quebrantamiento de las normativas y reglas establecidas.

[1] Los complejos de seguridad son un conjunto de unidades, cuyos mayores y principales procesos de securitización, desecuritización o ambos son tan interdependientes que sus problemas de seguridad no pueden ser razonablemente analizados o resueltos unos aparte de otros. (Buzan y Weaver 2004, págs. 44 – 45)

El proceso de securitización debe contemplar el análisis de los tipos de unidades que entran en esta dinámica. El primero de ellos son los objetos referentes, estos se constituyen como aquello que se encuentra amenazado y es vulnerable, por ejemplo la supervivencia de la población, la soberanía estatal, los ecosistemas, sistemas bancarios, entre otros. Los actores securitizantes se definen por los actores que perciben el problema y tratan de convertirlo en tema de seguridad, gobiernos, grupos sociales, individuos, organizaciones no gubernamentales. El último tipo de unidad que se presenta es el de los actores funcionales, los cuales afectan de manera positiva y negativa el proceso de securitización, estos pueden ser los causantes de la amenaza o simplemente actores que tienen intereses particulares frente al tema.

Para poder consolidar el proceso de securitización de un problema como amenaza a la seguridad nacional de uno o más gobiernos, se requiere del uso de herramientas discursivas que permitan exponer las razones y efectos de la amenaza, así mismo se buscan justificar las medidas y acciones que se van a implementar. Por último se busca conseguir la aceptación de la opinión pública y la población sobre la necesidad de hacer frente a las amenazas, así se vulneren los marcos legales establecidos. Es importante resaltar que no todos los problemas a la seguridad pueden securitizarse, en la medida que se estaría planteando una multiplicidad de factores que busquen este proceso. Por el contrario se determina la necesidad de utilizar los componentes establecidos en el proceso de securitización. Por tal motivo y para efectos de la investigación es importante cuestionarse acerca de la percepción de la amenaza del ciberterrorismo por parte de la Unión Europea.

El caso de la política de seguridad de la Unión Europea en términos de ciberseguridad se enmarcaba por el progreso de las tecnologías de la información y comunicación. Las amenazas percibidas en esta concepción se constituían por el uso malintencionado de las herramientas informáticas. Sin embargo esta percepción secundaria cambia transcendentalmente como consecuencia de los ciberataques con fines terroristas acontecidos en algunos Estados miembros de la Unión Europea, Estados Unidos y otros países del mundo. También se redefinen las prioridades de seguridad por la identificación del uso de los sistemas informáticos y de comunicación por parte de grupos terroristas.

Por consiguiente el fenómeno del ciberterrorismo entra en un proceso de securitización al interior de la Unión Europea. Este fenómeno se consolida como una amenaza existencial, que vulnera la seguridad nacional, supervivencia de la población, democracia, derechos fundamentales e imperio de la ley. En relación con el ciberterrorismo se puede analizar dicha perspectiva desde dos niveles de análisis, el nacional y regional. Dicha amenaza percibida o sufrida por los Estados genera procesos de securitización en la política doméstica, sin embargo al analizar las características de la amenaza se evidenció la necesidad de actuar en conjunto para proteger las redes de información, infraestructura crítica e infraestructura de información, dado que el ciberterrorismo presenta la particularidad de no tener límites ni fronteras. Por ende esta característica transfronteriza de la amenaza supone el análisis desde una perspectiva multidimensional.

El proceso de securitización en la Unión Europea incluye la intervención de su aparato institucional y la disposición de medidas y políticas especificas en los Estados miembros. Actualmente se adelanta un trabajo conjunto en la elaboración de políticas comunes que permiten mitigar y reducir el impacto de este fenómeno en la seguridad nacional y regional, dichas acciones determinadas por las disposiciones de seguridad colectiva en el seno de la UE.

Por tal motivo el concepto de securitización resulta indispensable para analizar los procesos que se han llevado a cabo en los Estados miembros, y dada la característica transnacional del fenómeno de ciberterrorismo evidenciar las acciones que se han generado en el seno de la Unión Europea. Esta amenaza ha motivado la creación de distintos marcos normativos que permitan establecer estrategias de lucha contra el fenómeno. De igual manera en la Unión Europea se han desarrollado mecanismos de defensa que integran las acciones estatales y las respuestas institucionales que garantizan el trabajo conjunto y reciproco entre los actores.

Sin embargo cabe resaltar que la securitización se consolida cuando se dan procesos de institucionalización al interior de los complejos de seguridad, este último nivel se determina por el entendimiento de los tomadores de decisión e instancias institucionales de hacer frente al problema securitizado y desarrollar políticas especificas en contra de la

amenaza existencial. Cabe resaltar que este proceso se desarrolla con base en la composición y estructura de los complejos de seguridad. Al finalizar este proceso se entiende que el problema o amenaza se considera como tema de seguridad. Por último, cuando el tema seguritizado deja de ser una amenaza existencial como consecuencia a los procesos y medidas institucionales implementadas, se presenta un escenario de desecuritización.

1.3. Niveles de análisis, variables y posibles evoluciones de un Complejo de Seguridad

Para poder lograr la compresión de los fenómenos de seguridad y garantizar la imparcialidad, el autor ofrece 4 niveles de análisis (Buzan y Weaver 2004, pág. 51): el nivel domestico, regional, interregional y global. Estos niveles permiten evidenciar como se desarrolla la relación entre los actores.

1. Nivel Domestico: este nivel hace referencia a las vulnerabilidades presentes en un Estado parte de una región. Se analizan las fortalezas y debilidades de acuerdo a la estabilidad del orden interno, como lo determina Buzan en términos de la correspondencia existente entre la Nación y el Estado. Las debilidades Estatales definen y evidencian los temores en materia de seguridad.
2. Nivel Regional: este nivel abarca las relaciones Estado- Estado y como estas configuran las regiones. Es por esto que se puede ubicar a la Unión Europea desde este nivel de análisis.
3. Nivel Interregional: se hace referencia a la relaciones entre diversas regiones vecinas. Cabe resaltar que este nivel es limitado dada las características del complejo que se definen por las relaciones internas. Sin embargo si las dinámicas de seguridad plantean la necesidad de entender el análisis de seguridad desde una óptica interregional, determinado por el cambio de la balanza de poder, influencia de potencias de una región a la otra y viceversa, este nivel de análisis cobra relevancia.
4. Nivel Global: este nivel hace referencia a las relaciones entre la estructura global y regional en materia de seguridad. Se analiza el rol que tienen los poderes globales en la región.

Barry Buzan denomina la unión de todos los niveles de análisis como la *Constelación de Seguridad*, esta se refiere a todas las relaciones e interacciones presentes en el análisis de seguridad, desde una perspectiva multisectorial y multiactoral.

A partir del conocimiento de los niveles de análisis de la teoría es necesario conocer su estructura esencial. Buzan establece cuatro variables que constituyen los complejos de seguridad. La primera de ella es la existencia de una frontera diferenciadora del complejo con sus vecinos. La segunda variable es la configuración de una estructura anárquica, que signifique la existencia de dos o más unidades autónomas dentro del complejo de seguridad regional. La tercera variable hace referencia a la polaridad, caracterizada por la distribución de poder entre las unidades preponderantes del complejo. La última variable da cuenta de los patrones de amistad y enemistad entre las unidades del complejo, estos patrones se presentan por medio de procesos de construcción social (Otálvaro 2006, pág. 236). Cabe resaltar que estas variables están sujetas a la voluntad de las unidades por conformar los complejos de seguridad regional, con el objetivo de reducir su vulnerabilidad y comprender las diferencias entre las unidades.

Buzan advierte que cualquier alteración en alguna de las variables modifica las dinámicas y estructura del complejo de seguridad. En consecuencia el autor plantea tres posibles escenarios de evolución de los complejos de seguridad regional.

> 1. Mantenimiento de statu quo: no se presentan cambios significativos en la estructura esencial de los complejos;
> 2. Transformación interna: se refiere a las variaciones en la frontera de los complejos de seguridad, este tipo de cambios afectan la estructura anárquica. Estos se pueden presentar por el desarrollo de procesos de integración, o por la distribución de poder entre las unidades ya sea por un proceso de desintegración, una conquista o tasas de crecimiento distintas entre las unidades. La transformación interna también puede presentarse cuando hay una variación entre los patrones de amistad-enemistad determinada por el surgimiento de nuevos liderazgos, nuevas concepciones ideológicas, discursos contradictores o amenazas de confrontación militar;
> 3. Transformación externa: se determina por la reconfiguración de las fronteras externas de los complejos de seguridad regional. esta transformación ocurre cuando se presenta una ampliación en las unidades de los complejos, así mismo se establece por la división de las unidades o por la aparición de nuevos complejos de seguridad. (Buzan y Weaver 2004, pág. 53).

En esta investigación cabe resaltar que este proceso de integración ya se constituyó en cuanto a la transformación interna, en la medida que se puede hablar de la Unión Europea como una comunidad de Seguridad, cuya característica principal se sustenta en el

establecimiento de un complejo de seguridad basado en la cooperación y análisis de las nuevas amenazas. Este proceso se consolida por el establecimiento de instituciones o procesos de integración que garanticen la protección de los Estados y ciudadanos frente a las nuevas amenazas como el ciberterrorismo.

1.4. Tipos de Complejos de Seguridad

Como resultado de las distintas variables, estructuras y niveles de análisis es posible tipificar los complejos de seguridad. El objetivo de Barry Buzan se centra en la identificación de tipologías específicas que den cuenta de las relaciones, características, dinámicas de amistad- enemistad y configuración de las interacciones entre las unidades de un complejo regional en materia de seguridad. Hay tres tipos de complejos de seguridad, estándar, centrado y con grandes poderes.

Los complejos de seguridad estándar: se caracterizan por tener una estructura anárquica, determinada por el entendimiento de las dinámicas de seguridad desde una óptica político-militar. El autor entiende este tipo de complejos desde la visión westfaliana de las relaciones internacionales. La distribución de poder está determinada por los poderes regionales, y pueden variar de una concepción unipolar dada la existencia de un solo poder en la región, a una configuración multipolar determinada por la existencia de más poderes. Barry Buzan advierte que en la concepción unipolar las dinámicas de seguridad no son controladas por este poder, y este no tiene la facultad de actuar de manera centralizada.

En los complejos de seguridad estándar no se identifican poderes globales, por esta razón las políticas de seguridad se determinan por la relaciones entre los poderes regionales. Esta interrelación entre los poderes regionales plantean los parámetros de actuación del resto de unidades de los complejos en materia de seguridad. La región puede constituirse con base a patrones de amistad- enemistad, balanzas de poder, alianzas entre las unidades, acuerdos y relaciones de entendimiento. Dado el proceso de constitución estos complejos de seguridad pueden presentarse como formaciones conflictivas, regímenes de seguridad o comunidades de seguridad (Buzan y Weaver 2004, pág. 55).

Complejos de seguridad centrados: la característica principal de este tipo de complejos se establece por el análisis y determinaciones en materia de seguridad desde un

ámbito central, ya sea por una potencia o por un centro institucionalizado. En los complejos de seguridad centrados se presentan tres posibles formaciones. Las dos primeras alternativas son de carácter unipolar, Grandes poderes (Rusia) y superpotencias (Estados Unidos). Estos poderes determinan las expectativas en materia de seguridad, por consecuencia los poderes regionales no tienen la capacidad suficiente para sobreponer la agenda. La dominación de la potencia global minimiza las posibilidades de las unidades del complejo.

La tercera forma de un complejo de seguridad centrado hace referencia a las regiones integradas por instituciones (Unión Europea). Dichas regiones se caracterizan por el entendimiento de las unidades en materia de seguridad, como consecuencia del desarrollo y establecimiento de una comunidad de seguridad. La centralización de la agenda de seguridad en el marco de instituciones permite consolidar los propósitos de las unidades como un conjunto, de igual medida permite que este complejo de seguridad se configure como una potencia con relevancia y legitimidad en el escenario internacional.

Complejos de seguridad con grandes poderes: la configuración de estos complejos está determinada por la presencia de dos o más poderes globales, cuyos análisis de seguridad influyen en el ámbito global. Los intereses de los poderes globales se reflejan en la concepción del complejo regional y global en materia de seguridad. Así mismo, los complejos de seguridad con grandes poderes intervienen en los procesos de seguridad de regiones contiguas, generando una interconexión entre distintas regiones, y posibilitando la ampliación del análisis de un complejo regional a otro. Este tipo de complejos pueden afectar la distribución de poder en las regiones, o en su defecto el establecimiento de la agenda de seguridad.

Con base en lo anteriormente expuesto se puede identificar a la Unión Europea como un ***complejo de seguridad centrado***, según el desarrollo teórico que se presenta este tipo de complejo de seguridad hace referencia a las regiones ya integradas por instituciones como la UE. Este tipo de integración se enmarca en la consolidación de los procesos de seguridad desde una perspectiva centralizada, determinada por la comunidad de seguridad. La Unión Europea como complejo de seguridad centrado toma la figura de representación internacional y encarna los intereses de seguridad de sus Estados miembros. Por tal razón,

la actuación de la UE en el marco de la lucha contra el ciberterrorismo se sustenta en distintas instituciones que determinan los lineamientos, procedimientos y estrategias que se deben seguir para poder hacer frente a este fenómeno.

La teoría de los complejos de seguridad regional establece la necesidad de estudiar las nuevas amenazas como el ciberterrorismo, ya que del entendimiento de estas se determinan las acciones y medidas que se deben establecer para mitigar su impacto en la seguridad nacional, regional e internacional.

2. CIBERTERRORISMO: FORMACIÓN, PARADIGMAS Y CAPACIDADES DE LA NUEVA AMENAZA

El fenómeno del ciberterrorismo se constituye como una nueva amenaza a la seguridad internacional, la definición del concepto se establece por la convergencia entre el ciberespacio y el terrorismo. Este capítulo expondrá las distintas dimensiones del ciberterrorismo, desarrollo, perpetradores, acciones pasadas, propósito del fenómeno, situación actual y vulnerabilidades, con el propósito de enmarcar y conceptualizar la complejidad del fenómeno.

De igual manera se buscan determinar los factores que motivan y explican este fenómeno, y así mismo las dimensiones que se desprenden como consecuencia de las acciones y modalidades del ciberterrorismo. Por esto resulta indispensable analizar el ciberterrorismo desde distintas perspectivas. La guerra en red como el primer momento de acceso de los grupos terroristas a los medios informáticos y de comunicación, el ciberterrorismo como nueva amenaza a la seguridad, las tácticas empleadas por grupos terroristas en el ciberespacio, los actos ciberterroristas que se han perpetrado, y la visión futurista sobre los posibles actos ciberterroristas.

Previamente a la explicación del fenómeno del ciberterrorismo es indispensable hacer la claridad sobre distintos conceptos que se presentan en esta temática, como lo son el cibercrimen y la ciberguerra. Ya que pueden llegar a confundir el objetivo de la investigación que se centra en el análisis del concepto de ciberterrorismo que hace referencia al uso del ciberespacio por parte de organizaciones terroristas con motivaciones y propósitos de índole política e ideológica. El concepto de cibercrimen puede relacionarse desde el delito económico, como el fraude informático, el robo, la falsificación, hacking a los sistemas computacionales, el espionaje informático, el sabotaje, el chantaje, la extorsión informática, la piratería entre otros crímenes que atentan contra la propiedad intelectual y material, la violación a la privacidad e intimidad, la distribución de contenidos informáticos ilegales y perjudiciales, la incitación a crímenes como la violencia sexual, racial u económica, que atentan contra la moralidad e integridad de las personas bajo una motivación económica mayoritariamente (Rodríguez 2007, pág. 9). Este tipo de actos se

relacionan al crimen organizado desde una óptica de ciberdelincuencia. Por otro lado la ciberguerra se posiciona en un ámbito estatal que se vale de las herramientas informáticas y del ciberespacio para poder alcanzar distintos propósitos.

> La ciberguerra puede ser entendida como una agresión promovida por un Estado y dirigida a dañar gravemente las capacidades de otro para imponerle la aceptación de un objetivo propio o, simplemente, para sustraer información, cortar o destruir sus sistemas de comunicación, alterar sus bases de datos, es decir, lo que habitualmente hemos entendido como guerra, pero con la diferencia de que el medio empleado no sería la violencia física sino un ataque informático que va desde la infiltración en los sistemas informáticos enemigos para obtener información hasta el control de proyectiles mediante computadores, pasando por la planificación de las operaciones, la gestión del abastecimiento, entre otros (Sánchez 2012, pág. 244).

Al tener claridad sobre los conceptos se puede afirmar que las herramientas y métodos de acción en el cibercrimen, la ciberguerra y el ciberterrorismo son similares y en algunos casos iguales, sin embargo la motivación de la perpetración de los actos es muy diferente. Es por esta razón que se consideró pertinente hacer la aclaración conceptual con el fin de comprender el fenómeno del ciberterrorismo desde la óptica de la motivación política, ideológica o religiosa que sustenta el propósito terrorista de generar terror en la sociedad y desestabilizar a los Estados, sin llegar a la equivocación de asemejar los conceptos de manera arbitraria.

Hecha la aclaración se puede determinar que en el proceso de identificación del fenómeno del ciberterrorismo se pueden identificar distintos momentos en torno a la aplicación del concepto, esto referido al devenir del fenómeno determinado por el desarrollo tecnológico y la globalización.

2.1. Guerra en red

Para el desarrollo de esta investigación se realizó un análisis histórico sobre el uso de los sistemas informáticos y de comunicación por parte de las organizaciones terroristas, con el objetivo de observar las dinámicas que se han presentado en el marco del desarrollo tecnológico y de los sistemas informáticos, y con el propósito de entender las dimensiones del fenómeno del ciberterrorismo en la actualidad.

Un primer momento que se puede determinar en la identificación del acceso de los grupos terroristas a las herramientas informáticas y de comunicación se presenta a

comienzos de los años 80 hasta finales de los 90. Este momento se puede evidenciar gracias al concepto de guerra en red de los autores John Arquilla y David Ronfeldt, en este momento histórico se evidencia el acercamiento de los grupos terroristas a los sistemas de información.

La guerra en red emanada de la era de la información permitió que los grupos terroristas aumentaran la capacidad de acción en materia de comunicación de manera más efectiva, ya que la revolución de la información aumentó la velocidad de la comunicación, redujo los costos para la comunicación, incrementó la banda ancha y expandió la conectividad por medio de la integración de la comunicación y las tecnologías computacionales (Zanini y Edwards 2001, pág. 35). De la misma manera se permitió el acceso directo a la población por medio de la difusión de información a escala global.

El término de guerra en red es el resultado del proceso de conceptualización de los retos y desafíos que se presentaron en la era de la información, sustentada en el desarrollo de nuevas tecnologías virtuales que permitieron la interconexión entre los distintos actores del sistema internacional.

> La Guerra en red es un concepto deducido- derivado de nuestro pensamiento sobre los efectos e implicaciones de la revolución de la información. Una vez acuñado el concepto, permite evidenciar el aumento de las formas de organización en red, y sobre todo la importancia de "las estrategias de información" y "las operaciones de información" a lo largo del espectro del conflicto, incluyendo grupos etno-nacionalistas, grupos terroristas, guerrillas, criminales y activistas (Ronfeldt 2013, pág. 19).

Los autores John Arquilla y David Ronfeldt definen la guerra en red como una nueva noción de conflicto en los diferentes niveles de la sociedad, distinto a las dimensiones estrictamente militares que se planteaban con la ciberguerra. La era de la información posibilitó la creación de distintas formas de organización y comunicación en red de pequeñas células terroristas que coordinaban y ejecutaban sus objetivos por medio del aprovechamiento de las nuevas tecnologías. Es así como los grupos terroristas incursionan en el escenario tecnológico y de revolución de la información como plataforma de lucha y consecución de objetivos políticos e ideológicos. El nuevo escenario de actuación de los actores que configuran el sistema internacional permitió la consolidación de medios de comunicación privados de grupos terroristas. El carácter de privacidad facilitó

los mecanismos de difusión de información, consecución de objetivos y reorganización de las estructuras tradicionales.

Adicionalmente, la era de la información permitió la aparición de distintas formas de confrontación entre actores no estatales y autoridades estatales en el marco de la actividad virtual. Dicho proceso aumentó la capacidad de acción e influencia de los grupos terroristas en la perpetración de la violencia y el terror en la sociedad. Lo anterior se explica por la redefinición de las estructuras determinadas por modelos de organización jerárquicas a formaciones de redes autónomas, las cuales accedieron a las distintas tecnologías de la información como: computadores, software, dispositivos de telecomunicaciones e internet con la finalidad de organizar y coordinar diversas actividades en pro del objetivo terrorista (Zanini y Edwards 2001, pág. 41). Estas nuevas estructuras se contraponen a la organización de los distintos sectores de defensa tradicionales, como la estructura militar que se establece por una concepción jerarquizada que implica el establecimiento de diversos procesos burocráticos, conductos regulares y polos de poder en el proceso de toma de decisión.

Los grupos terroristas dan uso de las ventajas operativas que se desarrollan en la era de la información dado que sus estrategias pueden ser empleadas de manera más eficaz y efectiva. La respuesta a dichas acciones se determina por los procesos y modelos tradicionales de defensa que no contemplan la reorganización de los grupos terroristas en redes informáticas, las nuevas herramientas de confrontación, y la efectividad y eficiencia del proceso de toma de decisiones. Por lo tanto la confrontación basada en términos militares y físicos transciende a un espectro complejo que aumenta los alcances de los grupos terroristas en la era de la información y desarrollo de internet.

Es por esto que resulta indispensable explicar el campo de acción de los grupos terroristas en la era de la información y en la configuración de nuevas dinámicas de conflicto en el sistema internacional (guerra en red), determinadas por el posicionamiento de los grupos terroristas en la red.

> La tecnología de la información también puede contribuir a mejorar la inteligencia, obtención y análisis de información por parte de grupos terroristas, también como las operaciones de información ofensivas. La capacidad por parte de un grupo terrorista de realizar operaciones informáticas ofensivas puede representar una amenaza significativa, dado que el mundo se ha vuelto más dependiente al flujo de la comunicación e información.

> Nosotros argumentamos que la era de la tecnología de la información puede ayudar a los grupos terroristas a llevar a cabo tres tipos de operaciones de información ofensivas. La primera enmarcada por el manejo de la percepción del grupo terrorista, que se complementa por las actividades de propaganda. Dicha tecnología puede ser utilizada con el propósito de atacar y perturbar distintos objetivos virtuales. Por último la tecnología de la información puede ser usada para causar destrucción física y material (Zanini y Edwards 2001, pág. 41).

Se plantean tres escenarios posibles para la ejecución de operaciones de información ofensivas por parte de grupos terroristas, operaciones sustentadas en el manejo de la información con fines desestabilizadores que atentan contra la seguridad estatal. La primera herramienta ofensiva que se plantea está relacionada con las tecnologías de la información, el objetivo terrorista se establece como una suerte de poder blando, con el propósito de influenciar en la percepción social que se posee del proyecto terrorista y la búsqueda de nuevos recursos de financiación. También se presenta la posibilidad del reclutamiento y adoctrinamiento terrorista por medio del uso de la información, esta herramienta mediática permite a los grupos terroristas ganar espacio en los medios de difusión de información y comunicación, visibilizando las estrategias y técnicas que se desarrollan en el seno del grupo terrorista.

Otro método de ataque utilizado por los grupos terroristas en contra de la información son los bloqueos a los sistemas computacionales, estas acciones electrónicas se fundamentan en aras de desestabilizar y permear la infraestructura virtual mediante el uso de técnicas de hacking como las bombas lógicas, la extracción de recursos monetarios y la modificación de información en los sitios web. Este tipo de acciones reflejan la posibilidad que tienen los grupos terroristas de ejercer influencia en la seguridad de los Estados sin necesidad de realizar acciones físicas. Las consecuencias se establecen por los estragos a los sistemas computacionales, la reducción de la velocidad de la red y el impacto económico de dichas operaciones de información ofensivas.

Finalmente, los terroristas adquirieron en la era de la información la posibilidad de realizar operaciones de información ofensivas de carácter destructivo, determinado por la capacidad de destruir y modificar los sistemas de información por medio del uso de distintos virus que alteran y modifican la información almacenada. Estas operaciones de información pueden resultar en pérdida de vidas humanas en la medida que los ataques

pueden ser dirigidos a la infraestructura crítica de un Estado (acueductos, control aéreo, transporte público).

Ahora bien, la evolución acelerada de las tecnologías y sistemas informáticos cambian las dinámicas de la guerra en red. A finales de la década de los 90's y a puertas del siglo XXI se presenta la transición de la era de la información sustentada por el desarrollo de internet a la era cibernética. Esta se define por la complejidad de relaciones entre las tecnologías informáticas y los actores que configuran el sistema internacional. Por tal razón los grupos terroristas pueden potencializar sus capacidades presentes en la guerra en red al escenario del ciberterrorismo, ya que sus estructuras organizacionales clásicas cambian hacia un esquema en red flexible y descentralizado (Molano 2009, Pág. 24).

2.2. Ciberterrorismo

A diferencia de la guerra en red en el ciberterrorismo se evidencia un proceso más complejo que no se limita exclusivamente a la comunicación e información, este momento es el resultado del proceso de evolución de las tecnologías y sistemas de información en el marco de la globalización. Sin embargo es importante resaltar que actualmente los grupos terroristas siguen utilizando las herramientas presentes en la guerra en red. Sumado a esto el desarrollo de los sistemas computacionales permitió la consolidación de un escenario virtual cada vez más interconectado, que cerró la brecha entre el mundo real y virtual.

Dicho escenario virtual global fue definido como el "ciberespacio", este concepto hace referencia al conjunto de relaciones virtuales y redes interconectadas por medio de tecnologías computacionales que reúnen a todos los actores virtuales del planeta tierra. El ciberespacio está compuesto por distintos actores como: el Estado, los gobiernos, sistemas financieros, infraestructuras de desarrollo, sectores de defensa, sociedad y todos los actores presentes en el mundo virtual. El ciberespacio se constituye como la plataforma de comunicación e interconexión de los actores presentes en la "red global", determinado por la dependencia en el flujo, automatización y control de la información.

Los grupos terroristas tienen un espectro más amplio de acción determinado por el ciberespacio, se presenta la comunicación en red, la planeación y perpetración de acciones sustentadas en los mensajes de terror, los procesos de reclutamiento, adoctrinamiento,

entrenamiento, difusión de información y ataques cibernéticos. Cabe resaltar que en los dos momentos que se explican la característica principal se enmarca en el objetivo terrorista de generar terror en la población, vulnerando las estructuras estatales e infraestructura crítica.

El fenómeno del ciberterrorismo se constituye como una amenaza reciente a la seguridad de los Estados y a los distintos actores del sistema internacional, para hablar de su conceptualización y origen podemos remontarnos a la década de los 80's cuando el investigador norteamericano Barry Collin denomina la correlación entre el terrorismo y el ciberespacio como ciberterrorismo, dicha relación estaba determinada por la complementariedad del ciberespacio como escenario favorable para perpetrar actos terroristas y en igual medida para servir de puente de acción de los grupos e individuos con fines terroristas. Sin embargo esta definición del concepto estuvo y continúa en constante construcción, Dorothy Denning, docente de la Universidad de Georgetown centra su definición en la motivación política del fenómeno y su finalidad de afectar considerablemente a la población o individuos, dichos actos ciberterroristas se desarrollan en detrimento de los sistemas económicos y de la vida humana.

> Cyberterrorism is the convergence of terrorism and cyberspace. It is generally understood to mean unlawful attacks and threats of attack against computers, networks, and the information stored therein when done to intimidate or coerce a government or its people in furtherance of political or social objectives. Further, to qualify as cyberterrorism, an attack should result in violence against persons or property, or at least cause enough harm to generate fear. Attacks that lead to death or bodily injury, explosions, plane crashes, water contamination, or severe economic loss would be examples (Denning 2003, párr. 1).

Esta definición refleja la complejidad del fenómeno del ciberterrorismo determinado por los distintos métodos de ataque, perpetradores, objetivos y estragos a la seguridad del los Estados y población vulnerable. Se determina entonces la convergencia entre el mundo cibernético y el objetivo terrorista, encaminado a vulnerar la seguridad de los Estados y a generar terror en la población mediante el ataque a estructuras de información virtual y a la infraestructura crítica de los Estados.

Resulta indispensable proporcionar otra definición que se ha desarrollado en el ámbito académico, cabe entonces resaltar la definición del profesor Mark Pollit de la Universidad John Hopkins, que comprende una concepción más técnica del

ciberterrorismo. En esta definición se comparte la motivación política del ataque ciberterrorista[2] el cual se desarrolla con base a una planeación y coordinación.

La definición que presenta el profesor Mark Pollit evidencia la naturaleza del fenómeno del ciberterrorismo como herramienta política y como instrumento al servicio de los grupos terroristas para perpetrar ataques premeditados con sustento político e ideológico, que conllevan a la generación de violencia.

Para entender la complejidad del fenómeno del ciberterrorismo es importante considerar los actores que realizan los actos "ciberterroristas" o ataques a los sistemas informáticos en nombre de la organización, en la medida que existe un desconocimiento o confusión con respecto a los artífices y responsables de dichos actos en el escenario del ciberterrorismo.

Es relevante hacer la aclaración que los actores informáticos que modifican y acceden a los sistemas computacionales tienen distintas motivaciones, no siempre de naturaleza terrorista. Pueden ser actores conocedores de los sistemas de información, individuos que por sus habilidades y capacidades pueden realizar acciones en la red que comúnmente usuarios a las tecnologías informáticas no dominan. Sin embargo la explicación se enmarca en la posibilidad de que los grupos terroristas influencien a estos actores para la consecución de sus objetivos en la red.

Los grupos terroristas buscan reclutar a dichos actores informáticos con el propósito de utilizar y aprovechar el conocimiento y habilidades de dichos agentes informáticos en la red. Sin embargo es importante resaltar que muchos de los ciberterroristas actuales fueron agentes informáticos comunes con intereses altruistas de conocimiento que simplemente cambiaron su objetivo por distintas motivaciones.

Los grupos terroristas en la era cibernética buscan consolidar ejércitos virtuales o de mercenarios que planeen, coordinen y ejecuten distintas acciones en la red, acciones encaminadas a consolidar los objetivos de los grupos terroristas. Por lo tanto los actores conocedores de los sistemas informáticos son fichas claves para los grupos terroristas. El

[2] Ataques premeditados y políticamente motivados en contra de información, sistemas computacionales, programas computacionales y datos, que resultan en violencia contra objetivos no combatientes por grupos sub-nacionales o agentes clandestinos (Krasavin 2012).

proceso de reclutamiento de estos agentes informáticos responde a distintas motivaciones de carácter político, ideológico, religioso o cultural, es en este momento donde se quebranta la delgada línea de acción entre un agente informático y un ciberterrorista.

Esta transición es sumamente peligrosa para la seguridad informática de los distintos actores del sistema internacional y en particular para la seguridad nacional de cualquier Estado, ya que el fenómeno del ciberterrorismo presenta la facilidad de ejercer acciones seguras, certeras y a bajo costo.

Los actores informáticos especializados y sobresalientes pueden ser vinculados a las filas terroristas bajo un discurso de beneficio personal y colectivo, en el ámbito de lo personal se apela a la posibilidad de conseguir recursos financieros por medio de la prestación de servicios informáticos a los grupos terroristas, dinero que motiva a los distintos agentes informáticos a realizar diversas acciones en la red sin conocer su razón de ser y sus consecuencias en el escenario político.

También se presenta la posibilidad de que los grupos terroristas vinculen a estos individuos por medio del adoctrinamiento ideológico, mecanismo que permite alienar los objetivos de los grupos terroristas y los agentes informáticos. La gravedad de esta motivación radica en que dichos actores informáticos cambian de percepción frente a los objetivos y razones que motivan su proceder en la red, se pasa de una motivación personal con propósitos de perturbación, humor y competitividad a una percepción política e ideológica que justifica las acciones violentas en la red que conllevan a la generación de terror en la sociedad. Esta motivación ideológica pretende que estos agentes redefinan su rol hacia una suerte de figura heroica que lucha por los propósitos del grupo que milita y que desenmascare los objetivos "perversos" de los Estados.

Otra razón que justifica la transición de estos actores hacia un espectro terrorista se desarrolla en el ámbito colectivo, ya que estos agentes buscan incasablemente su posicionamiento en las comunidades informáticas dada la característica anárquica del ciberespacio, y ya que el fenómeno del ciberterrorismo permite posicionar a los agentes informáticos como aquellos actores que vulneran las medidas de seguridad de los Estados. Es así que el posicionamiento de estos actores en las distintas esferas informáticas depende del alcance e impacto de las acciones que realicen.

Anteriormente se expusieron las motivaciones y posibles razones que tienen los agentes informáticos para convertirse en actores al servicio de los grupos terroristas, agentes que se denominaran como ciberterroristas. De igual manera se evidencia como las organizaciones terroristas persuaden a los distintos actores especializados en la red.

Si bien los grupos terroristas han enlistado a estos actores informáticos se presenta un desarrollo en la formación y educación informática al interior de la organización terrorista. Es entonces que encontramos una dualidad en la formación de ciberterroristas, la primera determinada por el reclutamiento de distintos individuos con capacidades sobresalientes en el dominio y entendimiento de los sistemas, y la segunda sustentada en la formación y entrenamiento de mercenarios informáticos en el seno del grupo terrorista.

La amenaza del ciberterrorismo a la seguridad nacional e internacional es latente, los actores que componen la estructura terrorista en la era de la informática permiten la consolidación de nuevas nociones de confrontación entre los Estados y las organizaciones terroristas, nociones que se caracterizan por el uso de instrumentos y herramientas novedosas que traslapan la confrontación del escenario real al virtual.

2.3. Tácticas del Ciberterrorismo

Las organizaciones terroristas han descubierto en la era cibernética distintas herramientas e instrumentos que permiten consolidar sus objetivos de manera más efectiva, eficaz y a bajo costo, por lo tanto es importante conocer los métodos utilizados por los grupos terroristas en el marco del ciberterrorismo. Sin embargo antes de enunciar las tácticas utilizadas por los grupos terroristas en la red, es indispensable analizar las razones que motivan a los grupos terroristas a perpetrar acciones contra el Estado y la sociedad por medio del uso de herramientas informáticas.

El aspecto económico juega un papel fundamental en el fenómeno del ciberterrorismo, los costos de las acciones terroristas son menores en la medida que no se requiere un alto grado de inversión para el desarrollo y ejecución de las actividades de terror. Este fenómeno modifica las estrategias utilizadas en el terrorismo tradicional que representan costos muy altos, por ejemplo: la compra de armas, creación de bombas y formación de ejércitos. En la era de la informática los grupos terroristas solo necesitan

poseer un computador, tener conexión a internet e invertir en el desarrollo de distintos virus y programas computacionales que desestabilicen o destruyan los sistemas informáticos.

Asimismo los ataques cibernéticos pueden ser dirigidos de forma anónima, los ciberterroristas acceden y crean cuentas con nombres y sobrenombres inventados, crean perfiles de información falsos que dificultan la identificación de los autores de los ciberataques por parte de las autoridades cibernéticas de los Estados. El factor del anonimato garantiza la protección de las identidades reales de los individuos terroristas y permite la difusión de información a gran velocidad. Lo anteriormente expuesto puede justificarse por la ausencia de mecanismos de control y regulación informática en los Estados.

Otra ventaja que poseen las organizaciones terroristas en el marco del ciberterrorismo está determinada por la multiplicidad de actores y blancos que pueden ser víctimas de sus ataques.

> La variedad y número de objetivos son enormes, el ciberterrorista podría atacar blancos de computadores y redes informáticas de los gobiernos, individuos, empresas de servicios públicos, compañías aéreas privadas, etc. La gran cantidad y complejidad de los posibles objetivos garantizan que los terroristas pueden encontrar debilidades y vulnerabilidades para explotar. Diversos estudios han mostrado que las infraestructuras criticas, tales como las redes de energía eléctrica y servicios de emergencia, puede ser vulnerables a los ataques ciberterroristas (Weimann 2004, pág. 6).

Son distintas las razones que motivan a los grupos terroristas a perpetrar actos por medio del uso de tecnologías informáticas. Como se ha explicado a lo largo de la investigación el ciberespacio y desarrollo tecnológico se han convertido en escenarios favorables para dichas organizaciones, sin embargo la efectividad de dichos ataques recae en la capacidad que poseen lo grupos terroristas. El Grupo de Monterrey (*Center for the Study of Terrorism and Irregular Warfare at the Naval Postgraduate School*) proporciona tres niveles que identifican la capacidad de los grupos terroristas en la perpetración de sus actos de acuerdo a su organización y estructura.

> - Capacidad Simple- Sin estructura, capacidad de conducir "Hacks" básicos contra sistemas individuales, utilizando herramientas creadas por alguien más. Las organizaciones poseen un nivel bajo de análisis del blanco (objetivo), control y comando, y mínima capacidad de aprendizaje.

- Capacidad Avanzada- Con estructura, capacidad de conducir ataques más sofisticados en contra de sistemas múltiples y redes, con la posibilidad de modificar o crear herramientas básicas de "hacking". La organización posee un nivel elemental de análisis del blanco, de igual modo sobre el control o capacidad de aprendizaje.
- Capacidad compleja- Coordinada, capacidad para un ataque coordinado que puede causar una irrupción masiva contra defensas integradas y heterogéneas (incluyendo la criptografía). Las organizaciones tienen la habilidad de crear herramientas de "hacking" sofisticadas. La organización posee un alto nivel de análisis del blanco, de igual modo sobre el control o capacidad de aprendizaje (Denning 2003, párr. 18).

Los niveles que presenta el Grupo de Monterrey son indispensables para analizar la capacidad que poseen los grupos terroristas en la perpetración de sus actos, se determina entonces la vulnerabilidad de los blancos de acuerdo a la capacidad de análisis y aprendizaje, y estructura que posea la organización. El conocimiento del objetivo, el aprovechamiento de herramientas informáticas desarrolladas por otros actores y por miembros de la organización, así mismo como el dominio y control sobre las acciones determina el éxito e impacto de las actividades de los terroristas en el ciberespacio.

Con lo anteriormente expuesto, resulta indispensable conocer las herramientas y métodos informáticos que se utilizan en las dinámicas del fenómeno del ciberterrorismo. Los ataques informáticos se definen como todas aquellas acciones que atentan contra los sistemas computacionales y de información, dichos actos tienen como propósito alterar, modificar y bloquear la información almacenada, el control del procesamiento y los equipos de operaciones informáticas.

Las herramientas utilizadas son diversas, determinadas por la vulnerabilidad del objetivo y del entendimiento y desarrollo de mecanismos sofisticados para el ataque. Cada ataque está supeditado a la capacidad de la organización terrorista, y a su vez a los mecanismos de defensa que poseen los blancos. Cabe resaltar que a lo largo del proceso académico de identificación del fenómeno del ciberterrorismo se han reconocido distintas herramientas de perpetración, por lo cual esta investigación retoma la conceptualización de Clay Wilson, Especialista en Tecnología y Seguridad Nacional, de la División de Comercio, Asuntos Exteriores y Defensa del Servicio de Investigación del Congreso de Estados Unidos. El cual presenta un análisis del fenómeno del ciberterrorismo desde los efectos de las herramientas o armas utilizadas. Se presentan entonces tres tipos de

herramientas para los ataques ciberterroristas, los ataques electrónicos, ataques a las redes computacionales y ataques físicos.

Los ataques electrónicos o armas de pulso electromagnético, son aquellas herramientas que utilizan y aprovechan el poder de la energía electromagnética, con el objetivo de afectar y/o destruir distintos sistemas informáticos. El uso del pulso electromagnético es indispensable para la perpetración del acto, este tipo de armas desestabilizan los equipos electrónicos, por medio de la descarga inmediata de energía electromagnética la cual sobrecarga los circuitos, afecta gravemente los transistores imposibilitando así la conducción y recepción de comandos. Igualmente las conocidas bombas lógicas pueden introducir códigos digitales maliciosos directamente en las ondas de transmisión, cabe resaltar que estas bombas lógicas no pueden ser consideradas como virus informáticos en la medida que no tienen la posibilidad de reproducción y autorregulación. Los efectos de estos ataques son altamente negativos para los sistemas informáticos, en la medida en que pueden conllevar a la eliminación de la memoria electrónica de los dispositivos, afectan igualmente el soporte lógico (software) del sistema informático que permite la realización de tareas especificas, también estos ataques pueden inhabilitar los componentes físicos (hardware) de un sistema informático.

Este tipo de herramientas requieren de un desarrollo avanzado por parte de las organizaciones que las emplean, distintas organizaciones terroristas no tienen la capacidad tecnológica para su desarrollo, no obstante el Departamento de Seguridad Nacional de Estados Unidos alerta sobre el riesgo y vulnerabilidad del sector público y privado, en la medida que Estados como Rusia y Estados patrocinadores del terrorismo señalados por la Secretaria de Estado de Estados Unidos desde octubre de 2004 entre los cuales se encuentran: Cuba, Irán, Irak, Libia, Corea del Norte, Siria y Sudán tienen la capacidad técnica de construir e implementar armas de pulso electromagnético (Adams 2003, párr. 17).

Ataques a las redes computacionales o Virus informático, este tipo de ataques cibernéticos están sustentados en programas informáticos o códigos maliciosos diseñados para ejecutar acciones específicas en contra de los sistemas informáticos interconectados por una red (Internet). Este tipo de ataques cibernéticos vulneran e inhabilitan información

almacenada, modifican los comandos de vigilancia y ejecutan comandos específicos para distorsionar y alterar redes informáticas u ordenadores específicos por medio del uso de internet. A diferencia de los ataques electrónicos estos programas tienen la capacidad y autonomía de propagarse, reproducirse y auto duplicarse (Bradley 2003, pág. 18).

Los ataques a las redes computacionales son los más utilizados por los ciberterroristas, Los cuales utilizan la interconexión del ciberespacio para perpetrar distintas acciones tales como, el acceso y sustracción de información privada, control remoto y dominio de los sistemas informáticos del objetivo, modificación y alteración de comandos específicos de los sistemas computacionales, bloqueo al acceso de los programas informáticos y la inhabilitación de los componentes lógicos de los sistemas.

Es importante aclarar que este tipo de herramientas en el ciberterrorismo son utilizadas gracias a la vulnerabilidad de los sistemas de defensa informáticos, conocidos como antivirus, sistemas de protección de información y dispositivos de bloqueo del acceso no autorizado (firewall).

En el fenómeno del ciberterrorismo este tipo de herramientas permite la consolidación de objetivos determinantes para los grupos terroristas. Dichas armas cibernéticas permiten la sustracción y alteración de información de seguridad nacional, de igual modo las organizaciones terroristas pueden sustraer recursos económicos para la financiación de las actividades. Otro escenario favorable para estas organizaciones es el espionaje de las actividades, programas e información sensible de los objetivos. Sin embargo la amenaza mayor se sustenta en la interferencia y alteración de las estructuras criticas del Estado, tales como las redes de energía, acueductos, plantas de tratamiento, control del tráfico aéreo y producción alimentaria, las cuales se encuentran automatizadas y estructuradas por programas y sistemas informáticos.

Ataques físicos, son todos aquellos actos que implican el uso de armamento convencional para desestabilizar o destruir los sistemas informáticos y los equipamientos que permiten su conexión, funcionamiento y control. Por ejemplo la creación de temperaturas altas que conllevan al daño de algunos componentes informáticos, así mismo la fragmentación de herramientas informáticas como cables de conexión, antenas, y demás artefactos que posibilitan la interconexión en red, emisión de frecuencias y señales.

Adicionalmente se pueden presentar situaciones de manipulación directa a los artefactos informáticos. Esta herramienta del ciberterrorismo se viene introduciendo en el ámbito académico desde hace poco tiempo, en la medida que se realiza el análisis del propósito y finalidad de los actos. Se evidencia la posibilidad de que los grupos terroristas utilicen armamento convencional para destruir y atacar equipamiento informático sensible y esencial para los Estados.

> En 1991, durante la Operación Tormenta del Desierto, los militares de EE.UU. interrumpieron las comunicaciones iraquíes y centros de cálculo mediante el envío de misiles de crucero a dispersar los filamentos de carbono generando un cortocircuito en las líneas de alimentación. Además, los ataques de Al Qaeda dirigidos contra el World Trade Center y el Pentágono el 11 de septiembre de 2001, destruyeron muchas bases de datos informáticas importantes y rompieron los sistemas financieros y de comunicaciones civiles y militares que estaban vinculados a nivel mundial. La pérdida temporal de los enlaces de comunicaciones y datos importantes, sumado a los efectos del ataque físico mediante el cierre de los mercados financieros durante un máximo de una semana (Wilson 2005, pág. 3).

Además de las tácticas de carácter técnico los grupos terroristas emplean tácticas de carácter logístico, estas determinadas por la multiplicidad de herramientas en el ciberespacio, objetivos fáciles de identificar, actuación en tiempo real y oportunidad de camuflaje en el entramado cibernético.

Es indispensable recordar que las organizaciones terroristas siguen utilizando los mismos métodos y propósitos presentes en la guerra en red, la revolución de la información sigue siendo un aliado clave en este fenómeno. La propaganda, difusión de información, consecución de recursos para el financiamiento de las operaciones y el reclutamiento, son herramientas utilizadas por los grupos terroristas, el desarrollo tecnológico plantea un escenario favorable para la consecución de los objetivos de dichos grupos.

Al igual que en la guerra en red pero con mayor efectividad los grupos terroristas hacen propaganda con la finalidad de instruir ideológicamente a los individuos, presentar los planes de acción y justificar las acciones y estrategias que se desarrollan. Este tipo de propaganda terrorista apela a las condiciones socio-económicas de la sociedad, utiliza discursos de reivindicación social en contra del sistema económico, religioso y cultural, y promueve el accionar violento como única salida a las dinámicas opresoras del sistema.

> Los contenidos pueden distribuirse ahora usando una amplia gama de herramientas, tales como sitios web especiales, salas virtuales de charla y foros, revistas en línea, plataformas de redes sociales como Twitter y Facebook, y sitios web populares de videos y de

> intercambio como Youtube y Rapidshare, respectivamente. El uso de los servicios de indización, como los buscadores de internet, también hace que sea más fácil descubrir y obtener contenido relacionado con el terrorismo. (Oficina de las Naciones Unidas contra la droga y el delito [UNODC] 2013, pág. 4).

El reclutamiento es la táctica que buscan engrosar las filas de los grupos terroristas, esta herramienta busca consolidar distintas células a lo largo del mundo que permitan el proceso de internacionalización de la organización.

> Investigadores de las Fuerzas de Seguridad y expertos académicos en el terrorismo yihadista consultados afirman que Internet es una poderosa herramienta de reclutamiento. La mayoría de grupos terroristas islamistas son muy conscientes de ese poder y realizan notorios esfuerzos para crear materiales audiovisuales susceptibles de ser cargados en la Red. Al Qaeda cuenta con su propia productora: As Sahab (las nubes) y Al Qaeda en el Magreb Islámico (AQMI) con la suya: Al-Andalus. En un principio, esas imágenes se difundían mediante cintas de vídeo que se visionaban en ambientes más bien cerrados-privados; pero el enorme poder de difusión de Internet y las dificultades para su control y restricción le han convertido en un instrumento verdaderamente idóneo para los fines del terrorismo yihadista, concretamente en sus labores de reclutamiento y captación (Delgado *s.f*, pág. 29).

Mediante el proceso de ingeniería social y estudio del objetivo se determinan los blancos vulnerables que son más proclives a introducirse en estas dinámicas. En este proceso se presenta la justificación y razones de la relevancia de enlistarse en la organización. Así mismo mediante la apelación a los sentimientos, inequidad social e inconformidades de los individuos se incita a la comisión de actos de violencia, por medio del adoctrinamiento ideológico, político o religioso. Se presenta un discurso de responsabilidad y de obligación de actuar para hacer frente a las condiciones y procesos desfavorables que se perciben. Este tipo de táctica es muy recurrente en las dinámicas del ciberterrorismo y en el propósito de ganar individuos que estén dispuestos a realizar acciones a cualquier nivel y a cualquier costo.

Los grupos terroristas buscan radicalizar el pensamiento de los individuos, moldeando sus preceptos y valores establecidos por premisas infundadas en procesos reivindicativos y contestatarios. A parte de esto los grupos terroristas usan las herramientas tecnológicas para adiestrar a los individuos en la consecución, planeación y coordinación de actos terroristas.

> Hay una gama cada vez mayor de medios de comunicación que proporcionan plataformas para la difusión de guías practicas en forma de manuales en línea, ficheros de audio y video, materiales de información y asesoramiento. Estas plataformas de Internet también ofrecen

> instrucciones detalladas, a menudo en formato multimedia de fácil acceso y en varios idiomas, sobre temas tales como la forma de afiliarse a organizaciones terroristas, cómo fabricar explosivos, armas de fuego u otras armas o materiales peligrosos, y cómo planear y ejecutar ataques terroristas (UNODC 2013, pág. 8).

Otra ventaja que tienen las organizaciones terroristas en la era cibernética son los métodos de financiamiento, hay una multiplicidad de formas para obtener recursos. Por medio de donaciones, sustracción ilícita de recursos financieros, establecimiento de paginas ficticias entre otras. Los grupos terroristas tienen la posibilidad de eliminar las fuentes de financiación tradicionales basadas en actos ilícitos, como el tráfico de drogas, armas, personas, extorsiones y demás delitos en el escenario real. Por lo tanto se reduce el riesgo de identificación y perdida de capital humano.

Las posibilidades de perpetrar actos terroristas en el ciberespacio son bastantes, las tácticas implementadas se determinan por la funcionalidad y objetivo que se resuelva en la organización terrorista. Ahora bien, es importante remontarnos y enunciar distintos actos ciberterroristas que se han presentado en el escenario internacional.

2.4. Actos ciberterroristas y posibles escenarios futuros

Partiendo del punto de construcción conceptual del fenómeno del ciberterrorismo es importante recordar distintos escenarios de acción en el que el ciberterrorismo se ha presentado. Uno de los primeros ataques ciberterroristas identificados fue la situación presentada en 1985 en Japón, en este suceso protagonizado por el grupo terrorista Middle Core Faction se vulneró y atacó el sistema de control de los ferrocarriles cortando el suministro de electricidad, efectuando el acceso a los cables de información de control de los ferrocarriles. También se perpetuó el acto terrorista interfiriendo en las comunicaciones de las autoridades pertinentes con el objetivo de entorpecer la respuesta. Este acto ciberterrorista afectó gravemente a millones de usuarios y dejó un efecto económico negativo a la compañía de trenes.

En la década del 90 el cibeterrorismo fue una herramienta de la organización tamil guerrillera de los Liberation Tigers, dicho grupo atacó a través de internet a distintas organizaciones del gobierno de Estados Unidos utilizando el método del mail bombing, evento que evidenció la vulnerabilidad de los sistema computacionales y de información

del país norteamericano. Otro ataque que sufrió Estados Unidos se dio en la Guerra del Golfo, ciberterroristas ingresaron a los servidores militares alterando los documentos médicos que contenían información vital para el desenvolvimiento de una confrontación militar.

El ciberterrorismo se ha presentado en distintos conflictos entre países europeos, los casos que se expondrán se enmarcan en el escenario de conflicto de los Balcanes y la disolución de la antigua Yugoslavia a principios de la década de los 90. La guerra entre Serbia y Croacia fue escenario del aparato ciberterrorista,

> El grupo de hackers serbios *Black Hand* ataca el Centro de Informática de Kosovo, universidades y la versión en línea del periódico *Vjesnik*. La respuesta croata es entrar en el sitio web de la Biblioteca serbia. *Black* Hand roba el fichero de contraseñas del Rudje Boskovic Institute como reacción. Seguidamente, los hackerscroatas se introducen en dos servidores serbios (Olvera y González 2012, párr. 4).

Se da entonces una arremetida de ataques cibernéticos que en gran medida intensificaron el conflicto. También el ciberterrorismo se presentó en la guerra de Kosovo (1996-1999), distintos hackers de Rusia, Yugoslavia y Estados Unidos invadieron las páginas virtuales con propaganda e información que incitó al conflicto, en dicho conflicto se transmitió propaganda negativa y se invadió la información de la Organización del tratado Atlántico Norte (OTAN) y de la misma manera se realizó hacia la parte de Yugoslavia. Cabe resaltar que Croacia esta en el proceso de adhesión a la Unión Europea y Kosovo es candidato a ser Estado miembro.

Otra acción que se identifica es el arresto de un hacker en España en el 2005, este sujeto atacó por internet al Departamento de Seguridad y Defensa de Estados Unidos vulnerando la seguridad de una base naval en donde se encontraba un dique de mantenimiento de submarinos nucleares. Con el evento anteriormente nombrado se observa como el ciberterrorismo carece de fronteras y como las dinámicas de ejecución van más allá del control de los Estados. Sumado a esto en el 2010 en España un alto funcionario de inteligencia afirma que el país se ha visto afectado por más de 80 ataques ciberterroristas a la infraestructura critica e instituciones gubernamentales.

Es imperante resaltar que aparte de estos actos ciberterroristas identificados distintas organizaciones terroristas a lo largo del mundo emplean herramientas informáticas como

páginas web (Ver Anexo 1), revistas en línea, diarios informativos, perfiles en redes sociales y mecanismos de comunicación. Al Qaeda, Hezbollah, IRA, Ejército rojo japonés, FARC, ETA, Partido Kurdo de los Trabajadores han desarrollado estrategias cibernéticas que posibilitan la ampliación, consolidación y éxito de su objetivo a la luz del desarrollo tecnológicos y de los sistemas informáticos.

A manera de ilustración distintas fuentes gubernamentales han identificado sitios de internet con vínculos y propósitos terroristas, que permiten la comunicación, información y planeación de distintas actividades en la red. Distintas plataformas facilitan la actuación de organizaciones terroristas en el ciberespacio. Por ejemplo alneda.com es la pagina web que contiene información encriptada de Al Qaeda por medio de la difusión de noticias, publicación de artículos y actividades de aplicación de la ley musulmana. Por su parte assam.com es el puente de comunicación de la yihad en Afganistán, Chechenia y Palestina. Sitios web como 7hj.7hj.com brindan adiestramiento a los cibernautas en la perpetración de ataques a los sistemas informáticos. También las páginas electrónicas aloswa.org y jihadunspun.net ofrecen contenidos de líderes terroristas como Osama Bin Laden, con el objetivo de incitar a la violencia y consecución de actos terroristas, bajo premisas de reivindicación religiosa y cultural (Thomas 2003, pág. 113).

La complejidad del fenómeno del ciberterrorismo genera diversos interrogantes sobre su alcance y futuro como amenaza a la seguridad internacional y nacional. La falta de predicción sobre el fenómeno propone un ambiente incierto, que cada vez más evidenciará las vulnerabilidades de los actores del Sistema Internacional.

El desarrollo tecnológico está en constante devenir, lo que implica la aparición de nuevas amenazas a la seguridad de los Estados en esta materia, por lo tanto es importante presentar distintas hipótesis que se han realizado en torno al posible desenvolvimiento futuro del fenómeno del ciberterrorismo. Sin embargo cabe resaltar que hay distintas posturas sobre el verdadero alcance del fenómeno, en la medida que hay un debate frente al impacto del ciberterrorismo como amenaza a la seguridad del los Estados, por lo cual se desprenden dos posturas enmarcadas en la amenaza existencial y el escepticismo frente al fenómeno. En esta investigación se analiza el riesgo inminente del fenómeno del ciberterrorismo como amenaza novedosa a la seguridad de los Estados.

El investigador Senior del Instituto de Seguridad e Inteligencia de California Barry Collin presenta distintos escenarios hipotéticos (Collin) que permiten evidenciar el alcance nefasto del ciberterrorismo. Dichos escenarios se plantean desde la vulnerabilidad de las estructuras críticas de los Estados.

- "Un ciberterrorista podría acceder remotamente a los sistemas de control de procesamiento de una planta elaboradora de cereales, cambiar los niveles de suplementación de hierro, y enfermar (e incluso eventualmente matar) a los niños de Estados Unidos mientras disfrutan de su desayuno. También podría realizar alteraciones similares en plantas de alimentos para bebés. La supuesta ventaja potencial para el ciberterrorista de este tipo de ataque es que no tendría que estar en la fábrica para ejecutar ese tipo de atentado.
- Un ciberterrorista podría interferir a los bancos, las transacciones financieras de dinero y los centros bursátiles. Esa manera, los habitantes del país perderían su confianza en el sistema económico. Dice Collin: ¿Se atrevería un ciberterrorista a intentar ingresar físicamente al edificio de la Reserva Federal, u otro equivalente? Difícilmente, desde el momento en que sería inmediatamente arrestado. Es más, un gran camión estacionado cerca del edificio sería detectado en forma automática. Sin embargo, en el caso de un ciberterrorista, el perpetrador podría estar sentado en otro continente mientras que los sistemas económicos de la nación colapsan, alcanzando una situación de desestabilización.
- Un ciberterrorista podría atacar a la próxima generación de sistemas de tráfico aéreo, y hacer que dos grandes aeronaves civiles choquen entre sí. Ese es un escenario realista, desde el momento en que el ciberterrorista también podría interferir los sensores del interior de la cabina. maniobras similares pueden ser realizadas con las líneas de ferrocarriles.
- Un ciberterrorista podría alterar las fórmulas de remedios o productos farmacéuticos, causando una gran cantidad de pérdidas humanas. Un ciberterrorista podría cambiar remotamente la presión de los gasoductos, causando fallas en las válvulas, y desencadenando una serie de explosiones e incendios. "De la misma manera, la red eléctrica se vuelve cada día más vulnerable" (Collin 1996, párr.10).

La interdependencia de la humanidad a las tecnologías de la información e informática hacen pensar en la posibilidad de cruzar la delgada línea entre lo hipotético y la realidad.

Para concluir y de acuerdo a las definiciones y análisis planteados por diversos ámbitos académicos se puede identificar el fenómeno del ciberterrorismo como una consecuencia del desarrollo tecnológico y de la información, así mismo como la herramienta ideal para la perpetración de actos terroristas y de ello la consecución del objetivo político y de generación de terror en la sociedad. El ciberterrorismo se constituye entonces como un referente novedoso de confrontación entre los grupos terroristas y los Estados, lo cuales se ven obligados a dar respuestas contundentes.

3. ACTUACIÓN DE LA UNIÓN EUROPEA EN CONTRA DEL FENÓMENO DEL CIBERTERRORISMO

La revolución informática y digital desencadenada del proceso del desarrollo tecnológico ha reconfigurado las capacidades, propósitos y objetivos de los actores que configuran el Sistema Internacional. Los fenómenos que resultan de la globalización plantean nuevos retos para la supervivencia y consecución de los intereses de las unidades que lo conforman.

Los eventos anteriormente expuestos permiten evidenciar el impacto y amenaza que representa el ciberterrorismo para la seguridad nacional e internacional. El resultado de esta nueva amenaza ha generado por parte de los Estados dinámicas cooperativas, que se determinan por el análisis y retos en materia de seguridad. Es por esta razón que en el seno de la Unión Europea se adelantan procesos de cooperación, fortalecimiento institucional, establecimiento de marcos legales a nivel nacional y regional con el objetivo de reducir las vulnerabilidades cibernéticas.

El objetivo de este capítulo es explicar las políticas, medidas de ciberdefensa y ciberseguridad, operaciones especiales y marcos jurídicos que se han creado en la Unión Europea y sus Estados miembros para mitigar el impacto del Ciberterrorismo en la región.

El modelo de la Unión Europea se constituyó como un hito sin precedentes en el sistema internacional. Los procesos de integración en el ámbito político, social y económico marcaron la pauta para el establecimiento de las relaciones del mundo globalizado. Este nivel de integración permite analizar de una manera más eficaz los problemas de seguridad nacional y regional, de ahí que el establecimiento de medidas en materia de seguridad recae en la funcionalidad del aparato institucional de la UE.

3.1. Instituciones de la UE encargadas de la ciberseguridad

La Unión Europea ha delegado el mandato en materia de ciberseguridad a distintas instituciones y organismos, los cuales tienen la responsabilidad de dar respuesta a las amenazas que se presentan desde un enfoque multidimensional. El fenómeno del ciberterrorismo requiere de un trato interinstitucional que permita abarcar la integralidad de

los supuestos que se presentan en este fenómeno. Las instancias políticas, de gestión y ejecución de la Unión Europea determinan las estrategias y marcos normativos que se desarrollan para minimizar el impacto de la amenaza, y poner fin a su influencia en las dinámicas de seguridad.

Para el análisis de la influencia del fenómeno del ciberterrorismo en la UE esta investigación distingue a las instituciones de acuerdo al rol que desempeñan. Primero se encuentran las instituciones que identifican la amenaza, segundo aquellas que introducen el tema en la agenda de seguridad, tercero las que formulan marcos normativos, estrategias y recomendaciones, y por último las encargadas del estudio, ejecución, control y seguimiento de las disposiciones que se determinen.

Bajo el análisis del ciberterrorismo se pueden identificar los siguientes aparatos institucionales. El Consejo Europeo puede ser considerado como la instancia política de más alto nivel, los dirigentes europeos plantean las preocupaciones y prioridades en materia de seguridad y la necesidad de abordarlas como tema prioritario en la agenda. El parlamento Europeo se consolida como la instancia democrática que expresa la voluntad de los ciudadanos europeos, esta tiene un carácter político, pero su funcionalidad se determina por la introducción del tema y poder legislativo. Por su parte el Consejo de la Unión Europea actúa como coordinador de temas específicos (Ciberseguridad), representado por expertos de cada Estado miembro, así mismo esta instancia política tiene un carácter legislativo. La Comisión Europea puede ser la instancia más importante en la securitización del fenómeno del ciberterrorismo en la UE, en la medida en que es la encargada de presentar los proyectos legislativos al Parlamento y Consejo, y vela por el cumplimiento de la legislación. La Comisión Europea desempeña los cuatro roles en el proceso de securitización puesto que evidencia la amenaza, la introduce, propone marcos legales y hace seguiemiento de los resultados legislativos.

La UE cuenta también con aparatos institucionales de carácter operativo, EUROPOL es la institución policial encomendada a apoyar procesos de fortalecimiento legal, investigación e inteligencia en materia de criminalidad. Para el propósito de la investigación desarrolla funciones en la lucha y prevención de terrorismo y en la seguridad cibernética determinada por el Centro Europeo del Cibercrimen. Eurojust es la institución

encargada de garantizar la cooperación en materia judicial, también el organismo se dota de facultades de investigación de los delitos cibernéticos y lucha contra el ciberterrorismo. ENISA (Agencia Europea de Seguridad de las Redes y de la Información) es la institución encargada de analizar las amenazas a los sistemas informáticos y buscar mecanismos que los protejan a través de la cooperación entre la UE y sus Estados miembros.

Las instituciones de la Unión Europea encargadas de analizar y contrarrestar los efectos del fenómeno del ciberterrorismo han entendido la importancia de la cooperación interinstitucional y de los Estados miembros. El éxito de las estrategias y políticas contra el ciberterrorismo se determinan por los mecanismos de diálogo y entendimiento entre los actores que participan en el proceso de securitización. Las instituciones de la UE tienen la tarea de concientizar a los distintos sectores de la sociedad sobre los riesgos y amenazas que se presentan. El discurso securitizador debe estar encaminado a la aprobación y comprensión de la medidas que se apliquen en contra de este fenómeno, así vayan en detrimento de los marcos legales establecidos.

El fenómeno del ciberterrorismo ha requerido de la utilización del entramado institucional de la Unión Europea. La complejidad del fenómeno conlleva al establecimiento de dinámicas interinstitucionales de carácter político, social, económico y cultural en el seno de la UE y en el nivel domestico de sus Estados miembros.

3.2. Respuesta de la Unión Europea

Compartiendo la amenaza común que representa el fenómeno del ciberterrorismo y gracias al proceso de securitización se han generado distintas acciones en el escenario regional y nacional. En el seno de la Unión Europea se ha establecido un marco normativo que protege a Europa de los ciberataques y que blinda las infraestructuras críticas de los Estados miembros. A continuación se enunciaran las acciones de mayor relevancia que se han llevado a cabo en la UE con el propósito de consolidar políticas de protección contra el ciberterrorismo.

Como primer momento nos remontamos a la decisión del Consejo Europeo en diciembre del 2001, en esta decisión se sientan las bases en torno a las medidas requeridas para la lucha contra el ciberterrorismo y así mismo se definen las características y alcances

del terrorismo. Como resultado de un consenso se determina la necesidad de proteger las infraestructuras críticas de los Estados incluyendo los sistemas de información.

Un aporte fundamental que se dio en el marco del establecimiento de parámetros claros sobre la ciberseguridad fue la Convención de cibercriminalidad de Budapest del 2001. Esta convención se constituyó como el primer aporte normativo en la Unión Europea que delimitaba los alcances de las amenazas a la seguridad cibernética. Se determinaron las medidas que deberían adoptarse a nivel nacional, se suministró terminología esencial para el análisis del fenómeno, se presentaron modelos en materia de derecho penal y procesal, y se enmarcó la importancia de la cooperación internacional en materia de ciberseguridad. Distintos Estados del mundo se adhirieron a esta convención dada la importancia de generar parámetros de análisis entorno a las amenazas presentes en el ciberespacio. Actualmente 14 Estados miembros de la UE han ratificado la convención.

Una respuesta importante del Consejo Europeo es la decisión marco de junio de 2002 en la lucha contra el terrorismo, en esta decisión se establece la posibilidad y obligación de los Estados miembros de generar acciones internas que permitan adecuar distintas normativas contra el terrorismo, tipificando los daños y consecuencias de este fenómeno. La elaboración de políticas nacionales se corresponden por medio de la cooperación entre los Estados miembros. De la misma manera se evidencia la importancia de atacar las acciones terroristas en contra de los sistemas informáticos desde las dimensiones nacionales y regionales.

Otra decisión relevante contra el ciberterrorismo se presenta con la creación de la Agencia Europea de Seguridad de las Redes y de la Información (ENISA) en marzo del 2004 en el marco de decisión del Parlamento Europeo. La creación de esta agencia permite consolidar una institución encargada de la seguridad de las redes de información y sistemas informáticos. Así mismo esta agencia surge con el objetivo de fortalecer los mecanismos de defensa cibernética por medio del establecimiento de una instancia de alto nivel que promueve estrategias de cooperación y protección dentro de la Unión Europea.

El 24 de febrero de 2005 se presenta una decisión marco del Consejo, que se refiere a la posibilidad de ataques ciberterroristas contra los sistemas de información e infraestructuras vitales de los Estados miembros. En este momento se plantea la posibilidad

de que los Estados intervengan en el control de los sistemas de información, dada la posibilidad de acceso y uso de estos mecanismos de información por parte de grupos terroristas.

En complemento en mayo de 2005 se elaboró la Convención del Consejo de Europa para la prevención del terrorismo. En este convenio se establecen las medidas para prevenir el terrorismo y hacer frente a la provocación de cometer actos terroristas. También se refiere a las políticas nacionales que se deben implementar para la prevención del terrorismo, determinadas por la cooperación de las autoridades nacionales. En cuanto al ciberterrorismo se puede decir que este instrumento analiza los nuevos métodos y técnicas de reclutamiento y adoctrinamiento utilizadas por los grupos terroristas. Es importante resaltar que solo 6 Estados miembros (Bulgaria, Croacia, Dinamarca, Eslovaquia, Finlandia y Rumania) de la UE han ratificado este instrumento.

Es importante resaltar que la Unión Europea ha venido desarrollando distintos programas que protegen las infraestructuras críticas de los Estados, la UE define infraestructura crítica como:

> Aquellas instalaciones, redes, servicios y equipos físicos y de tecnología de la información cuya interrupción o destrucción tendría un impacto mayor en la salud, la seguridad o el bienestar económico de los ciudadanos o en el eficaz funcionamiento de los gobiernos de los Estados miembros (Comisión al Consejo y al Parlamento Europeo 2010, párr. 5).

Dichas infraestructuras críticas son altamente vulnerables a ataques por parte de grupos terroristas. Es por esto que en el 2008 se crea el Programa para la protección de las infraestructuras críticas de la Unión Europea.

En el 2010 el Consejo de la UE presenta la Estrategia de Seguridad Interior de la Unión Europea "Hacia un modelo europeo de seguridad" (Ver Anexo 2) para el periodo 2010-2014. Esta estrategia evidencia las amenazas y desafíos comunes de la UE, plasma los principios y política común de seguridad interior, por lo cual plantea el modelo de seguridad Europea. Dicha estrategia identifica las amenazas recurrentes, entre ellas el terrorismo en cualquiera de sus manifestaciones (ciberterrorismo).

> El terrorismo, en cualquiera de sus formas, tiene un desprecio absoluto por la vida humana y los valores democráticos. Su alcance global, sus consecuencias devastadoras, su capacidad de reclutamiento a través de la radicalización, así como la difusión de propaganda a través de Internet y los diferentes medios a través de los que se financia, hacen del terrorismo una

> amenaza significativa y en constante evolución para nuestra seguridad (Consejo Europeo 2010, pág. 13).

Se identifica la ciberseguridad como prioridad en la estrategia. Este documento presenta algunas respuestas a los desafíos de seguridad, entre los que se encuentran: la anticipación a las amenazas, la planificación, programación y gestión de medidas, la efectividad del trabajo de las agencias, instituciones y organismos de la UE, la cooperación a nivel institucional y nacional, y el diseño de mecanismos de evaluación de las estrategias aplicadas.

Con el objetivo de fortalecer los mecanismos y estrategias en contra del ciberterrorismo, en el 2011 el Consejo Europeo crea el Comité de Expertos en Terrorismo (CODEXTER). Esta instancia intergubernamental elabora perfiles de los Estados en relación a su capacidad de respuesta al terrorismo, Igualmente promueve el intercambio de información y la aplicación de prácticas exitosas en la materia. Este comité identifica las fallas del derecho internacional referidas al terrorismo, por lo que tiene la facultad de presentar propuestas en materia de lucha contra el terrorismo.

Otra determinación importante encaminada a fortalecer los marcos legales y jurídicos en la prevención y lucha contra el ciberterrorismo, se da gracias al establecimiento del Centro Europeo del Cibercrimen en 2013, en el marco institucional de EUROPOL. Este centro es la instancia preponderante en la lucha contra el cibercrimen en la UE, ya que brinda apoyo y acompañamiento a los Estados miembros en materia de investigación y construcción de políticas y estrategias que garanticen la protección de los sistemas informáticos, infraestructuras criticas y redes de información.

El último instrumento que se ha establecido en la UE es la Estrategia de Ciberseguirdad de la Unión Europea del 2013 (Ver Anexo 3). Este documento reafirma los principios y objetivos que se tienen en el marco de la protección de la sociedad, infraestructuras críticas de los Estados, sistemas informáticos y de información. Se resalta la aplicación de los valores de la UE en el ámbito digital como en el escenario físico, se promueve la protección de los derechos fundamentales, la libertad de expresión y la privacidad de la información personal. Entre tanto se enuncia la importancia de la cobertura y acceso, democracia, gobernanza eficiente y la responsabilidad compartida para garantizar

un escenario cibernético seguro. La estrategia de ciberseguridad tiene 5 prioridades estratégicas:

> La ciberresiliencia; la reducción drástica de la delincuencia en la red; el desarrollo de una política de ciberdefensa y de las capacidades correspondientes en el ámbito de la Política Común de Seguridad y Defensa (PCSD); el desarrollo de los recursos industriales y tecnológicos necesarios en materia de ciberseguridad; el establecimiento de una política internacional coherente del ciberespacio en la Unión Europea y la promoción de los valores europeos esenciales (Comisión Europea 2013, pág. 4).

Los aportes de la Estrategia de Ciberseguridad son esenciales para la consolidación del análisis y entendimiento de la problemática del ciberterrorismo. Cuando se habla de ciberresiliencia se busca promover en los individuos procesos de concientización sobre los riesgos del ciberespacio y el impacto que genera en la seguridad nacional, protección de los sistemas informáticos y de información, las infraestructuras criticas del Estado y hasta la supervivencia de la población.

Para alcanzar los objetivos en materia de seguridad cibernética la Unión Europea ha establecido canales de comunicación y cooperación a nivel bilateral y multilateral, esto con el objetivo de abarcar los retos de manera integral dada la característica transnacional del ciberterrorismo. Estas relaciones entre los diversos actores del sistema internacional garantizan la coordinación de políticas y estrategias desde el mutuo entendimiento de los desafíos y amenazas que se presentan a la seguridad Estatal y global. A nivel bilateral la UE ha profundizado la cooperación técnica y táctica con Estados Unidos, representada en el establecimiento del Grupo de Trabajo de la Ciberseguridad y el Cibercrimen. Adicionalmente en el plano multilateral la UE ha participado activamente en diversos foros internacionales de toma de decisión, tales como la Asamblea General de Naciones Unidas, la Unión Internacional de Telecomunicaciones, la Organización para la Cooperación y el Desarrollo Económico (OCDE), la Cumbre Mundial sobre la Sociedad de la Información, La Organización Europea de Seguridad y Cooperación (OSCE) y el Foro sobre Gobernanza del Internet (Comisión Europea 2013).

Así mismo, es de suma importancia resaltar las relaciones profundizadas en materia de Seguridad cibernética entre la UE y la Organización del Tratado del Atlántico Norte (OTAN), en la medida en que se han construido estrategias conjuntas de ciberseguridad,

entre las que sobresalen el intercambio de información, los procesos de investigación, entrenamiento y educación, la cooperación e instauración de alianzas con los sectores industriales y privados. Estas estrategias permiten integrar el tema cibernético en la agenda estratégica de defensa y seguridad de la UE y la OTAN.

Se destaca que la lucha contra el ciberterrorismo que adelanta la UE se sustenta en la cooperación con los distintos órganos policiales, instituciones nacionales, regionales e internacionales que garantizan el éxito en las acciones que se emprenden en contra de este fenómeno. Es por esto que cada vez más se intensifican las medidas entorno a la consolidación de sistemas de información seguros, acciones de respuesta extraordinarias, coherentes y efectivas que afronten de manera integral las dinámicas complejas que se presentan con el ciberterrorismo.

3.3. Respuesta de los Estados Miembros

El éxito en la lucha de un fenómeno transnacional como el ciberterrorismo requiere de la implementación de medidas a nivel nacional que involucren a todos los sectores de la sociedad. El entendimiento de las disposiciones a nivel institucional debe guiar la hoja de ruta en la coordinación, gestión, ejecución y complementariedad de las medidas.

El Comité de Expertos en Terrorismo (CODEXTER) realizó un análisis acerca de los países miembros de la Unión Europea que han desarrollado marcos normativos y legales contra el fenómeno del ciberterrorismo. La investigación se realizó a 20 países miembros de la UE[3]. Los resultados fueron determinantes, de los 20 Estados analizados solo 7 Estados (Alemania, Bélgica, Dinamarca, Estonia, Lituania, Rumania y Reino Unido) tienen marcos legales concretos que criminalizan o evidencian de forma directa la actividad ciberterrorista. Estos Estados tienen elementos referentes al fenómeno del ciberterrorismo, con instrumentos legales específicos o tipificaciones en sus códigos penales. Sin embargo la mayoría de Estados de la Unión Europea abordan el fenómeno desde la interpretación de sus marcos legales y jurídicos de ciberdefensa y ciberseguridad, esta interpretación de las

[3] Los Estados son los siguientes: Alemania, Austria, Bélgica, Chipre, Croacia, Dinamarca, Eslovaquia, España, Estonia, Finlandia, Francia, Hungría, Letonia, Lituania, Luxemburgo, Países Bajos, Portugal, Reino Unido, República Checa, Rumania y Suecia.

leyes existentes busca disponer del aparato legal, normativo y jurídico de los Estados para hacer frente al fenómeno y amenaza del ciberterrorismo.

A manera de ilustración, Alemania ha establecido la Política "Anti-terror", instrumento normativo que criminaliza los actos ciberterroristas, esta política busca desmantelar toda red informática terrorista por medio de procesos de investigación que reducen la capacidad operativa de los perpetradores. Así mismo este instrumento previene las amenazas terroristas, y se enmarca en un proceso reciproco de cooperación internacional. Las acciones que han realizado las instituciones alemanas buscan prevenir y educar a la población, con el fin último de eliminar las causas del terrorismo, y comprender la complejidad del fenómeno del ciberterrorismo.

Es importante resaltar que distintos países miembros como: Bélgica, Dinamarca, Letonia y Holanda siguen los lineamientos de la Convención de Cibercrimen de Budapest de 2001, los marcos legales se establecieron con base en la hoja de ruta que presentó la Convención, y se observan procesos de adecuación de políticas internas referentes al particular.

Igualmente es importante resaltar que Estados como: España, Francia, Hungría, Lituania, Holanda, Portugal, República Checa y Suecia presentan marcos jurídicos y códigos penales que hacen referencia al uso malintencionado del ciberespacio por grupos terroristas. En la actualidad los Estados miembros de la Unión Europea tienen parámetros legales que evidencian las dinámicas peligrosas del ciberterrorismo. Los enfoques y medidas adoptadas en el seno de la Unión Europea encaminan a los Estados miembros a establecer y propiciar marcos jurídicos, estrategias y políticas que protejan al Estado y población de la amenaza inminente del ciberterrorismo.

3.4. La Unión Europea en busca del establecimiento de una política concreta contra el Ciberterrorismo: *"Clean It Project"*

A pesar de todas las estrategias y políticas que se han establecido en el seno de la UE para hacer frente al fenómeno del ciberterrorismo distintos Estados miembros han expresado la necesidad de promover un diálogo de alto nivel sobre las medidas específicas que se deben implementar en contra del ciberterrorismo, y sobre la importancia de incluir a todos los

sectores de la sociedad en la educación, prevención y protección del uso del ciberespacio por parte de organizaciones terroristas. El *"Clean It Project"* es una iniciativa de la Unión Europea financiada por la Comisión Europea, bajo el liderazgo de Holanda, Bélgica, Alemania, Reino Unido y España, y que cuenta con el apoyo de Hungría, Rumania e Italia.

Entre el 2011 y 2013 se llevaron a cabo distintas reuniones de alto nivel entre distintos actores del ámbito público y privado, en torno a la necesidad de abordar el tema del uso de internet por parte de grupos terroristas en la agenda de seguridad de la UE. De estas reuniones se plantearon distintas recomendaciones encaminadas a dificultar e imposibilitar el accionar terrorista en la red. Se planteó la necesidad de involucrar a las compañías privadas de internet en la protección de los usuarios, y así mismo en la identificación de posibles usos malintencionados de la red. De igual forma se estableció la necesidad de crear un mecanismo de alerta para que los usuarios puedan reportar y denunciar cualquier acción sospechosa en redes sociales, sitios de foros, páginas web, correos electrónicos, que den cuenta de procesos de reclutamiento, adoctrinamiento, propaganda y planeación de actividades terroristas.

Este tipo de recomendaciones requieren del fortalecimiento e instauración de marcos legales que permitan a los Estados luchar en contra de los ciberterroristas. Igualmente la cooperación entre los Estados y las compañías de internet son fundamentales para minimizar los riesgos, dichas compañías tienen la responsabilidad de retirar de sus dominios contenidos pro terrorista y de responder diligentemente a las denuncias y notificaciones entabladas por los usuarios.

La estrategia de "*Clean it Proyect"* posibilita a los Estados y a las compañías de internet a intervenir de forma directa en la red, por medio del establecimiento de campañas de concientización sobre los riesgos que plantea el fenómeno, y así mismo sobre la responsabilidad que tienen los ciudadanos con la seguridad cibernética y nacional de los Estados. Este tipo de recomendaciones han generado polémica alrededor de varios sectores de la sociedad, ya que contempla la violación de derechos fundamentales, y da pie a la utilización de estas políticas para otros fines diferentes al propósito establecido.

La iniciativa "*Clean It Project"* de la UE se presenta como la primera alternativa de discusión sobre el fenómeno del ciberterrorismo, sin embargo este diálogo de alto nivel

logrará constituirse en una política específica de ciberseguridad por medio del entendimiento de las voluntades políticas, económicas y sociales en la UE que determinen la urgencia de una actuación multidimensional y multisectorial frente al ciberterrorismo. De no ser así se continuará con la interpretación de los marcos legales existentes en materia de ciberseguridad en la Unión Europea y sus Estados miembros. Los Estados que lideran esta iniciativa buscan utilizar todos los mecanismos de negociación y cooperación para pasar de la esfera retorica a la práctica, con la finalidad de establecer el proyecto *"Clean it"* como política de la Unión Europea.

4. CONCLUSIONES

Las amenazas a la defensa y seguridad nacional producto del fenómeno del ciberterrorismo han obligado a la Unión Europea a disponer de todas sus capacidades en materia de ciberdefensa para mitigar el accionar de las organizaciones terroristas. Es por esto que cada vez más se intensifican las acciones en el seno de la Unión Europea dada la posibilidad del accionar terrorista por medio del uso del ciberespacio.

Los procesos de toma de decisión a nivel nacional y regional se determinan por el establecimiento de dinámicas discursivas comunes, que evidencian el riesgo que representa el fenómeno del ciberterrorismo, la complejidad del fenómeno ha obligado a la Unión Europea a tomar decisiones integrales que se ajusten a los desafíos en materia de ciberseguridad. Sin embargo como se logró evidenciar en la investigación pocos Estados miembros han aplicado políticas específicas contra el fenómeno, lo que podría producir un debilitamiento de las políticas regionales. La actuación en contra del fenómeno del ciberterrorismo debe realizarse con base a un principio de reciprocidad, al mismo modo que se debe buscar replicar las experiencias exitosas de los Estados miembros que han tipificado el fenómeno en sus marcos legales y normativos.

Igualmente y con base en la investigación realizada se puede denotar que la Unión Europea ha establecido múltiples escenarios de defensa contra las amenazas del ciberterrorismo. Pero es mínima o casi nula la referencia específica de algún marco institucional de la Unión Europea por crear una política particular y estrictamente referida al ciberterrorismo. Hasta el año 2013 se comienzan a esbozar pequeños esfuerzos de distintos países de la Unión Europea por crear un documento único y referente al ciberterrorismo, esto referido al proyecto “Clean It”.

Los Estados deben evitar la interpretación de los actos terroristas desarrollados en el ciberespacio como una reinterpretación legal y jurídica de la lucha contra el terrorismo tradicional. Esto se sustenta en la necesidad de crear un análisis concreto al campo de batalla de los ciberterroristas. Puesto que resulta complicado y peligroso replicar las acciones que se realizan en el ámbito físico y real al plano virtual. Aunque se hace la

salvedad que en términos del derecho penal y procesal si se puede imputar y juzgar a los ciberterroristas bajo la misma vara del terrorismo tradicional.

A lo largo de la investigación se explicó consistentemente las características, desafíos y concepción actual del fenómeno del ciberterrorismo, por lo cual el análisis de seguridad que ha venido implementando la Unión Europea se determina por las herramientas y mecanismos de seguridad que deben estar presentes para la protección de la población, infraestructuras críticas, sistemas informáticos y estabilidad estatal. Es así que se puede identificar a la Unión Europea como una ***comunidad de seguridad*** altamente integrada, La teoría de Buzan permite hacer un análisis del ciberterrorismo como fenómeno contemporáneo en las dinámicas de seguridad nacional y transnacional, lo cual se evidencia en la consolidación de acciones y políticas conjuntas que logran disminuir el impacto del fenómeno en la seguridad regional. La trascendencia de dicha amenaza generó el fortalecimiento en los procesos de integración en materia de seguridad cibernética en el seno de la Unión Europea.

El status de la amenaza del ciberterrorismo en los niveles de análisis de seguridad europea se puede identificar como un proceso de securitización fuertemente establecido y en desarrollo. Pero que requiere del fortalecimiento discursivo de la ciberresiliencia en los distintos sectores de la sociedad, para que se justifiquen y comprendan las medidas que se toman y que pueden estar en detrimento de los estándares legales y derechos fundamentales tales como la libertad de expresión y de acceso a los medios informáticos.

Es por esto que esta monografía concluye afirmando que los procesos en materia de análisis de seguridad de la Unión Europea en el marco del ciberterrorismo deben vigorizarse, por medio del establecimiento de medidas particulares y endémicas del fenómeno en el ámbito nacional y en el fortalecimiento de las posiciones por parte de la UE. Con el objetivo de transcender hacia la constitución de una política clara y definida que dé cuenta de procesos de desecuritizacion del fenómeno y que posicione a la UE como actor internacional que fija los parámetros de la ciberseguridad y la lucha contra el ciberterrorismo en el mundo.

BIBLIOGRAFÍA

Arquilla, J., y Rondfelt, D. (2001). *Networks and Netwars: The Future of Terror, Crime, and Militancy.* Disponible en: http://www.rand.org/pubs/monograph_reports/MR1382.html

Buzan, B., y Weaver, O. (2004). *Regions and Powers. The Structure of International Security*, Cambridge, Cambridge University Press.

Buzan, B. (1991). *People, States and Fear*. *An Agenda for International Security Studies in the Post-Cold War Era*. Segunda Edición. Colorado, USA: Lynne Rienner.

Buzan, B., Weaver, O., y de Wilde, J. (1998). *Security: a new framework for analysis*. USA: Lynne Rienner Publishers.

Capítulos y Artículos

Buzan, B., y Weaver, O. (2004). Levels: distinguishing the regional from the global. En Buzan, B., y Weaver, O. *Regions and Powers. The Structure of International Security.* (págs. 27-40). Cambridge: Cambridge University Press.

Buzan, B., y Weaver, O. (2004). Security Complexes: A theory of regional security En Buzan, B., y Weaver, O. *Regions and Powers. The Structure of International Security.* (págs.40-82). Cambridge: Cambridge University Press.

Buzan, B., y Weaver, O. (2004). Theories and histories about the structure of contemporary international security En Buzan, B., y Weaver, O. *Regions and Powers. The Structure of International Security.* (págs.6-27). Cambridge: Cambridge University Press.

Buzan, B. (1991). National and International Security: The Policy Problem. En Buzan, B. *People, States and Fear.* (págs.328-360). Hertfordshire: Harvester Wheatheaf.

Buzan, B. (1991). Regional Security. En: Buzan, B. *People, States and Fear.* (págs.186-226). Hertfordshire: Harvester Wheatheaf.

Buzan, B., Weaver, O., y Wilde, J. (1998). Introduction. En: Buzan, B., Weaver, O., y Wilde, J. *Security. A New Framework for Analysis.* (págs.1-21). Colorado: Lynne Rienner Publishers.

Zanini, M., Edwards, S. (2001). The Networking of Terror in the Information Age. En: Arquilla, J., y Rondfelt, D. *Networks and Netwars: The Future of Terror, Crime, and Militancy.* (págs. 29-60). Disponible en: http://www.rand.org/content/dam/rand/pubs/monograph_reports/MR1382/MR1382.ch2.pdf

Artículos en publicaciones periódicas académicas

Cujabante, X. (2013). Mercosur: un análisis desde los complejos de seguridad. *Revista científica General José Maria Córdova*, 11(11), 99-120. Disponible en: http://www.esmic.edu.co/esmic/images/Publicaciones/2013/11/Revista%20cientifica.pdf

Thomas, T. (2003). Al Qaeda and the Internet: the Danger of "Cyberplanning". *Parameters, ProQuest Military Collection*, 33, 112-123. Disponible en: http://strategicstudiesinstitute.army.mil/pubs/parameters/articles/03spring/thomas.pdf

Molano, A. (septiembre, 2009). Terrorismo camaleónico: evolución, tendencias y desafíos inminentes del terrorismo global. *Revista Fuerzas Armadas*, 81 (211), 20-27. Disponible en: http://www.cgfm.mil.co/CGFMPortal/Cgfm_files/Media/File/pdf/Revista%20FFAA%202009/EDICION%20211.pdf

Otálvaro A. (2006). La seguridad internacional a la luz de las estructuras y las dinámicas regionales: una propuesta teórica de complejos de seguridad regional. *Revista Desafíos, Universidad del Rosario*, 11, 222-242. Disponible en: http://revistas.urosario.edu.co/index.php/desafios/article/view/669/599

Rogríguez, A. (2007). Los cibercrímenes en el espacio de libertad, seguridad y justicia. Revista de Derecho Informático, 103, 1-42. Disponible en: http://www.egov.ufsc.br/portal/sites/default/files/los_cibercrimenes_en_el_espacio_de_libertad_seguridad_y_justicia.pdf

Sánchez, G. (2012). Cibercrimen, ciberterrorismo y ciberguerra: Los nuevos desafíos del siglo XXI. Revista Cenipec, 31, 241-267. Disponible en: http://www.saber.ula.ve/bitstream/123456789/36770/1/articulo9.pdf

Wilson, C. (2005). Computer Attack and Cyber terrorism: Vulnerabilities and Policy Issues for Congress. Congressional Research Service Report for Congress. Disponible en: http://www.history.navy.mil/library/online/computerattack.htm

Otros documentos

Adams, M. (31 de octubre de 2003). The Dawn of the E-Bomb. IEEE Spectrum Online. Disponible en: http://www.spectrum.ieee.org/WEBONLY/publicfeature/nov03/1103ebom.html

Bradley, A. (2003). Anatomy Of Cyberterrorism Is America Vulnerable. Air War College. Air University, Maxwell Field. Disponible en: http://www.au.af.mil/au/awc/awcgate/awc/ashley.pdf

Consejo De Europa. (2012). Clean It Project. Detailed recommendations document for best practices and permanent dialogue. Disponible en: http://www.edri.org/files/cleanIT_sept2012.pdf

Collin, B. (1996). The Future of CyberTerrorism: Where the Physical and Virtual Worlds Converge. 11th Annual International Symposium on Criminal Justice Issues. Institute for Security and Intelligence. Disponible en página web: http://www.crime-research.org/library/Cyberter.htm

Comisión Europea. (20 de octubre 2010). Comunicación de la Comisión al Consejo y al Parlamento Europeo: Protección de las infraestructuras críticas en la lucha contra el terrorismo. Disponible en: http://eur-lex.europa.eu/legal-content/ES/ALL/;jsessionid=GTkhTR2GYYjh4mt1MVJSSBRvmCg2XhdWpm1WSQ06T8YFW08QGy6h!-692944551?uri=CELEX:52004DC0702

Comisión Europea. (2013). Directiva del Consejo y Parlamento Europeo: Concerning Measures to ensure a high common level of network and information security across de Union. Disponible en: file:///C:/Documents%20and%20Settings/Usuario/Mis%20documentos/Downloads/ProposalforaDirectiveoftheEuropeanParliamentandoftheCouncilconcerningmeasurestoensureahighcommonlevelofnetworkandinformationsecurityacrosstheUnion-COMfinal--EN.pdf

Comisión Europea. (febrero de 2013). European Union: External Action. Plan de ciberseguridad de la UE para proteger una red abierta plena de libertad y de

oportunidades en línea. Comunicado de prensa. Disponible en: http://europa.eu/rapid/press-release_IP-13-94_es.htm

Consejo De Europa. (2001). Convención de cibercriminalidad de Budapest. Disponible en: http:///conventions.coe.int/Treaty/en/Treaties/Html/185-SPA.htm

Consejo De Europa. (2005). Convención del Consejo de Europa para la prevención del terrorismo. Disponible en: http://www.boe.es/boe/dias/2009/10/16/pdfs/BOE-A-2009-16476.pdf

Consejo Europeo. (2010). Estrategia de Seguridad Interior de la Unión Europea Hacia un modelo europeo de seguridad 2010-2014. Disponible en: https://www.consilium.europa.eu/uedocs/cms_data/librairie/PDF/QC3010313ESC.pdf

Consejo Europeo. (2013). Estrategia de Ciberseguirdad de la Unión Europea. Disponible en: file:///C:/Documents%20and%20Settings/Usuario/Mis%20documentos/Downloads/CybersecurityStrategyoftheEuropeanUnionAnOpenSafeandSecureCyberspace-JOINfinal-%20(2).pdf

Conway, M. (2002). Reality Bytes: Cyberterrorism and Terrorist Use of the Internet. Department of Political Science of Trinity College. Dublin. Disponible en: http://doras.dcu.ie/498/1/first_mon_7_11_2002.pdf

Delgado, F. (*s.f.*). El reclutamiento del terrorismo Yihahista. Disponible en: http://www.asociacion11m.org/contenidos/recortes/45.pdf

Denning, D. *(s.f.).* Federation of American Scientists. Disponible en: http://www.fas.org/irp/congress/2000_hr/00-05-23denning.htm

Denning, D. (Mayo de 2003). Terrorist Threats to the United States. Statement House Special Oversight Panel on Terrorism. Disponible en: http://www.fas.org/irp/congress/2000_hr/00-05-23denning.htm

Krasavin, S. (2012). Computer Crime Reasearch Center. Disponible en: http://www.crime-research.org/library/Cyber-terrorism.htm

Oficina de las Naciones Unidas contra la droga y el delito. (2013). El uso de internet con fines terroristas. Disponible en: http://www.unodc.org/documents/terrorism/Publications/Use_of_Internet_for_Terrorist_Purposes/Use_of_Internet_Ebook_SPANISH_for_web.pdf

Olvera, G. Belén, M. y González Cerrato, J. (16 de enero de 2012). Dossier sobre ciberterrorismo. Red Hispanoamericana de Análisis de la Seguridad Global. Disponible En: http://www.redsafeworld.net/news/dossier-sobre-ciberterrorismo-monica-belen-olvera-gorts-y-juan-carlos-gonzalez-cerrato-/

Weimann, G. (Diciembre 2004). United States Institute of Peace. Special Report. Cyberterrorism: How Real Is the Threat. Disponible en: http://dspace.cigilibrary.org/jspui/bitstream/123456789/15033/1/Cyberterrorism%20How%20Real%20Is%20the%20Threat.pdf?1

Anexos

Anexo 1. Tabla. Secretaria de Estado de los Estados Unidos de América. "Sitios Web de Organizaciones Terroristas 2002".

Organisation	URL**	Language(s)
1. Abu Nidal Organisation (ANO)	N/A	N/A
2. Abu Sayyaf Group (ASG)	N/A	N/A
3. Al-Aqsa Martyrs Brigade	N/A	N/A
4. Armed Islamic Group (GIA)	N/A	N/A
5. Asbat al-Ansar	N/A	N/A
6. Aum Supreme Truth (Aum)	http://www.aleph.to/index_e.html http://www.aleph.to	English Japanese
7. Basque Homeland and Liberty (ETA)	http://www.contrast.org/mirrors/ehj/index.html http://www.batasuna.org/	English Basque
8. Al-Gama'a al-Islamiyya (Islamic Group)	http://www.azzam.com	English
9. Hamas	http://www.palestine-info.com/hamas	Arabic, English
10. Harakat ul-Mujahidin (HUM)	http://www.ummah.net.pk/harkat/	Arabic, English
11. Hizbollah	http://www.hizbollah.org	Arabic, English
12. Islamic Movement of Uzbekistan	N/A	N/A
13. Jaish-e-Mohammed	N/A	N/A
14. Al-Jihad (Egyptian Islamic Jihad)	N/A	N/A
15. Kahane Chai (Kach)	http://www.kahane.org	English
16. Kurdistan Workers Party (PKK)	http://www.pkk.org/index.html	Kurdish
17. Lashkar-e-Tayyiba	http://www.markazdawa.org.pk/	Arabic, English
18. Liberation Tigers of Tamil Eelam	http://www.eelamweb.com/	English
19. Mujahedin-e Khalq Organization	http://www.iran-e-azad.org/english/index.html	English
20. National Liberation Army (ELN), Colombia	http://www.eln-voces.com/	Spanish
21. Palestine Islamic Jihad (PIJ)	http://www.entifada.net/	Arabic
22. Palestine Liberation Front (PLF)	N/A	N/A
23. Popular Front for the Liberation of Palestine (PFLP)	http://www.pflp-pal.org/main.html	English
24. Popular Front for the Liberation of Palestine- General Command (PFLP-GC)	N/A	N/A
25. al-Qaida	http://www.alneda.com	Arabic
26. Real IRA	N/A	N/A
27. Revolutionary Armed Forces of Colombia (FARC)	http://www.farc-ep.org/	English, Spanish, Portuguese, Italian, German, Russian
28. Revolutinary Nuclei (formerly ELA)	N/A	N/A
29. Revolutionary Organization 17 November (17 November)	N/A	N/A
30. Revolutionary People's Liberation Party/Front (DHKP/C, Dev Sol)	http://www.ozgurluk.org	English
31. Salafist Group for Call and Combat	N/A	N/A
32. Sendero Luminoso (Shining Path)	http://www.csrp.org/	Spanish, English
33. United Self-Defense Forces of Colombia (AUC)	http://colombia-libre.org/colombialibre/pp.asp	Spanish

Fuente: (Conway 2003, pág. 4)

Anexo 2. Documento. Unión Europea. "Estrategia de Seguridad Interior de la Unión Europea "Hacia un modelo europeo de seguridad 2010-2014"

Fuente: (Consejo de Europa 2010, págs. 7-30).

Disponible en: https://www.consilium.europa.eu/uedocs/cms_data/librairie/PDF/QC3010313ESC.pdf

Anexo 3. Documento. "Estrategia de Ciberseguridad de la Unión Europea del 2013"

Fuente: (Comisión Europea 2013, págs. 2-20).

Disponible en: file:///C:/Documents%20and%20Settings/Usuario/Mis%20documentos/Downloads/CybersecurityStrategyoftheEuropeanUnionAnOpenSafeandSecureCyberspace-JOINfinal-%20(2).pdf