r.esici.9(18):225-242,2017

El terrorismo en la era de la información[1]

Edilmer Mejía Saldaña[2, *]
Daniel Molano Villanueva[3, **]

Resumen

El presente artículo es el resultado final del proyecto de investigación "Transformaciones del terrorismo en la era de la información", desarrollado en el contexto del Observatorio de Geopolítica y Seguridad Internacional de la Facultad de Relaciones Internacionales de la Escuela Militar de Cadetes "General José María Córdova". Este proyecto emergió a partir de la preocupación que se deriva del uso que hacen de las tecnologías de la información y la comunicación las organizaciones terroristas, que han evolucionado para adaptarse a la era de la información desde la cual sus actividades representan una mayor amenaza para los Estados y la seguridad internacional. A su vez, las nuevas tecnologías también han modificado el funcionamiento y la estructura de los grupos terroristas que han asumido el modelo red, más descentralizado y flexible.

Desde esta perspectiva, el lector podrá encontrar en el presente artículo una síntesis de la era de la información como proceso histórico que transformó todas las actividades humanas, incluyendo la guerra y el terrorismo, lo que conlleva al análisis del ciberterrorismo como una nueva amenaza para la seguridad internacional que opera de manera descentralizada, flexible y compleja bajo el modelo de la guerra en red descrito por John Arquilla y David Ronfeldt. A partir de allí, el lector conocerá las

[1] Artículo de Investigación.

[2] Internacionalista de la Escuela Militar de Cadetes "General José María Córdova".

[*] edimer_ms91@hotmail.com.

[3] Internacionalista de la Escuela Militar de Cadetes "General José María Córdova".

[**] dani_molano13@hotmail.com.

Fecha de recepción:
10 de marzo de 2016.

Fecha de aprobación:
3 de agosto de 2016.

Para citra este artículo:
Mejía, E. y Molano, D. (2017). El terrorismo en la era de la información. *Perspectivas en intgeligencia, 9*(18): 225-242.

diferentes tácticas y acciones que desarrollan los ciberterroristas en internet, que superan el robo de información de seguridad nacional y el ataque a la infraestructura crítica, al incluir la propaganda ideológica, el reclutamiento y la coordinación de actos terroristas en el mundo real.

Palabras clave: terrorismo; internet; ciberterrorismo; guerra en red; nuevas tecnologías.

Clasificación JEL: F51, F52, L86, L63.

Abstract

The present article is the final result of the investigation project named "Transformations of terrorism in the information age", developed within the context of the Geopolitics and National Security Observatory from the International Relations Faculty located at Escuela Militar de Cadetes "General José María Córdova". This project emerged based on a concern generated against the actual use of information and communications technologies coming from terrorist organizations, which have evolved to adapt to the information age, point at which their activities represent a greater threat for the States and national security. At the same time, new technologies have modified the functionality and the structure of terrorist groups that have assumed the net model, more decentralized and flexible.

From this perspective, the reader will be able to find within this article a synthesis about the information age as a historical process that transformed all of human activities, including war and terrorism, entailing an analysis of cyber terrorism as a new threat towards an international security operating in a decentralized manner, flexible, and complex under the net model described by John Arquilla y David Ronfeldt. Departing from that point, the reader will find different tactics and actions developed by cyber terrorist across the Internet, which surpass national security's information theft and also the attack towards critical infrastructure, when it comes to include ideological propaganda, recruitment and coordination from terrorist actions in the real world.

Keywords: terrorism; cyber terrorism; Internet; net war; new technologies.

JEL classification: F51, F52, L86, L63.

Introducción

El presente artículo es el resultado final del proyecto de investigación "Transformaciones del terrorismo en la era de la información", desarrollado en el contexto del Observatorio de Geopolítica y Seguridad Internacional de la Facultad de Relaciones Internacionales de la Escuela Militar de Cadetes "General José María Córdova". Este proyecto emergió a partir de la preocupación que se deriva del uso que hacen de las tecnologías de la información y la comunicación las organizaciones terroristas, que han evolucionado para adaptarse a la era de la información desde la cual sus actividades tienen mayor impacto cualitativo y cuantitativo. A su vez, las nuevas tecnologías también han modificado el funcionamiento y la estructura de los grupos terroristas que han asumido el modelo red, más descentralizado y flexible.

Bajo esta dinámica, el creciente uso de la internet y demás tecnologías de la información de los grupos terroristas en todo el mundo demanda una respuesta académica que permita comprender las dinámicas subyacentes a este hecho, lo que implica analizar información sobre cómo funciona la era de la información, qué motivaciones encuentran los grupos terroristas para actuar en la internet, qué beneficios obtienen en comparación con el viejo mundo sin estas tecnologías y, finalmente, qué hacen los Estados para neutralizar las actividades de estas organizaciones en la internet.

En tal sentido, se advierte que el ciberterrorismo, como concepto que busca explicar el uso de las tecnologías de la información y la comunicación de los actores terroristas, no se limita a los ataques contra la infraestructura crítica conectada a la red o el robo de información de seguridad nacional. De hecho, el ciberterrorismo, como concepto, comprende todas las actividades de estas organizaciones delictivas en las que se emplean las nuevas tecnologías, ya sea para hacer difusión de sus ideales, reclutar nuevos miembros, comunicar asuntos internos de la organización y coordinar ataques en el mundo real.

En efecto, la transformación del terrorismo en el siglo XXI demuestra que el ciberterrorismo es catalogado como nueva amenaza a la seguridad nacional y, por tanto, es y seguirá siendo durante los años venideros una tarea que los Estados deberán afrontar en cualquier parte del mundo donde se presente el fenómeno. Al mismo tiempo, al ser una amenaza que va de la mano con las tecnologías informáticas, su transformación y evolución es bastante acelerada, lo que demanda que las autoridades nacionales e internacionales estén en constante labor de estudiar y comprender el fenómeno. Pero más complejo aún, se trata de combatir un terrorismo que se ha "desterritorializado", aludiendo

a la idea de que si bien aquellos que componen las estructuras de estos grupos se encuentran geográficamente posicionados en un plano real, su capacidad de adaptar prácticas en la virtualidad les ha permitido extender el terrorismo al mundo entero, gracias a las nuevas tecnologías.

De esta manera, el primer reto en materia de investigación consistió en identificar las características de la era de la información, en el sentido de cómo las nuevas tecnologías transformaron todas las actividades humanas, incluyendo la guerra. Desde allí, se continuó con una conceptualización de la guerra en red y la guerra en enjambre como modelos explicativos sobre la forma como las nuevas tecnologías transformaron el funcionamiento y la estructura de las organizaciones terroristas, al hacerlas más descentralizadas, flexibles y complejas. Posteriormente, se abordaron las principales actividades de los actores terroristas con base en las nuevas tecnologías de la información.

Materiales y métodos

Para la investigación se planteó una metodología que permitiera abarcar las diferentes necesidades de recolección y organización de la información. Al respecto, la metodología documental-cualitativa favoreció una revisión extensa sobre la guerra en red, como paradigma básico de interpretación sobre cómo la era de la información ha modificado la estructura y la operatividad de las organizaciones terroristas y, a partir de allí, caracterizar el ciberterrorismo y sus principales actividades en internet.

Para realizar la revisión documental, la investigación se centró en la información de fuentes abiertas disponible en bases de datos académicas como ProQuest, EBSCO, Dialnet y Redalyc. De igual manera, se obtuvo información de centros de investigación en seguridad y defensa, como el Real Instituto Elcano, el Instituto Español de Estudios Estratégicos, RAND Corporation, entre otros. La información obtenida en estas fuentes fue organizada y analizada acorde con las siguientes variables:

1. Características de la era de la información, la guerra en red y la guerra en enjambre.
2. Características del terrorismo antes de las tecnologías de la información.
3. Características del ciberterrorismo como nueva amenaza a la seguridad internacional.
4. Principales actividades de los actores ciberterroristas en internet.

La era de la información: terrorismo, guerra en red y nuevas tecnologías

Para comprender el fenómeno del ciberterrorismo, primero es necesario realizar una aproximación teórica y conceptual a la era de la información, como contexto general en el que se desarrolla esta nueva amenaza para la seguridad internacional. Al respecto, se emplea el principal autor en la materia, Manuel Castells, quien describió cómo las innovaciones en la tecnología de la información permitieron a la sociedad organizarse en torno a un sistema de redes que facilitaron, en todo el sentido, las actividades cotidianas de la humanidad (Castells, 1999: 29).

En este mismo orden, también se debe tener en cuenta a autores como John Arquilla y David Ronfeldt (2001: 33), quienes plantean que la organización en red de los diferentes procesos sociales solo es posible gracias a las tecnologías de la información y la comunicación. En este contexto, la guerra, como proceso social, no escapa a este fenómeno, de ahí que los autores argumenten un cambio sustancial en la naturaleza de los conflictos armados, en tanto las nuevas tecnologías permiten a las organizaciones terroristas renovar su modo de operar, tanto en internet como en la vida real (Arquilla y Ronfeldt, 1997: 15). Según Manuel Castells (2001),internet se puede considerarcomo "el tejido de nuestras vidas dada su capacidad para distribuir el poder de la información por todos los ámbitos de la actividad humana" (p. 8).

Esto se debe a que la introducción de tecnologías de la información y la comunicación, con base en la informática, y en especial internet, permite que las redes desplieguen su flexibilidad y adaptabilidad, afirmando así su naturaleza evolutiva, permitiendo la coordinación de tareas y la gestión de la complejidad (Castells, 2001: 34). De esta manera, la eficacia a la hora de realizar tareas es mayor, debido al incremento de la capacidad de coordinación que se tiene al momento de ejecutar funciones individuales que al final hacen parte de un sistema complejo.

Desde esta perspectiva, los Estados y demás actores del sistema internacional usan las redes cibernéticas para manejar sus infraestructuras críticas, como instalaciones, redes, servicios, equipos físicos, entre otros, lo que ha generado una gran dependencia de las nuevas tecnologías, en especial en las sociedades más desarrolladas (UNODC, 2013: 12). Esta dependencia que han generado los Estados de las nuevas tecnologíasles exige enfrentarse a nuevas amenazas que surgen, gracias a las facilidades que otorga la organización de las redes, en este caso terroristas, al tiempo que estas redes fueron evolucionando en la medida

en que se revolucionaba el mundo con la manera de compartir la información. Ahora los grupos terroristas se integran dentro de redes, dejando a un lado la organización jerárquica y alterando una característica central de la naturaleza de los conflictos (Arquilla y Zanini, 2001: 13).

En efecto, las tecnologías de la información y la comunicación han otorgado a las redes terroristas una ventaja a la hora de la ejecución de sus actos violentos. Hoy en día los grupos terroristas, como cualquier otra organización, han asumido nuevas maneras de organizarse y han cambiado su modo de operar (Laqueur, 1999: 258). Por tal motivo, Arquilla y Zanini (2001b) caracterizan estos grupos como organizaciones en red, que "operan en pequeñas unidades dispersas sobre el territorio y que se despliegan con rapidez en cualquier lugar y en cualquier momento" (p. 9).

Según la teoría de la guerra de redes, gracias a la fácil compartimentación de la información, estos grupos terroristas pueden organizarse en red, lo que les permite ser más flexibles y adaptables a las condiciones de la guerra irregular frente a un oponente militar más poderoso, tal como se describió anteriormente. De este modo, los grupos terroristas asumen una formación de red en todos los canales, que hace referencia a que cada uno de los individuos o grupos de la organización están enlazados entre sí y pueden compartir información unos con otros. En consecuencia, ya no es necesario que estén todos atrincherados en los mismos lugares, es decir, ya no se mueven en grandes masas, se manejan pequeñas células que enlazadas comparten la información necesaria para estar al tanto de todo y logran descentralizar el mando de la organización (Arquilla y Ronfeldt, 1996: 21).

Esta misma descentralización permite a las células de la red terrorista tener iniciativa propia y actuar por sí solas. Esto se logra cuando cada una de las células o determinadas células de un sector posee un líder, la organización de la red de todos los canales comúnmente pierde su cabeza principal, aunque esto no quiere decir que la organización terrorista desaparezca; a cambio de ello, las células adoptan un comportamiento más regional y se dispersan por el territorio, pero siguiendo siempre los mismos intereses e ideales que los identifican (Arquilla y Zanini, 2001: 11).

Esta es la nueva era de la información, en la que quien logre controlar las ventajas de comunicación, maleabilidad y adaptación que ofrece la red, tendrá la ventaja sobre el adversario. En este sentido, ya no se trata de tener el mayor potencial bélico, sino de lograr controlar las fuentes de información, lo que conlleva a la guerra de redes, modelo que asumirán muchos de los actores no

estatales que desde los atentados del 11 de septiembre amenazan la seguridad internacional (Sánchez, 2010: 23); esta nueva organización les brindará la ventaja de romper su esquema jerárquico y ampliar y diversificar la capacidad de acción terrorista.

Ante esta nueva situación, Arquila y Ronfeldt (1996: 17) resaltan que la guerra en red no solo se basa en el uso de Internet. Es verdad que las nuevas tecnologías facilitaron mucho la organización de las redes, pero estas pueden existir apoyándose en viejos instrumentos de comunicación, como los correos humanos y una correcta combinación entre los sistemas antiguos y los nuevos. La guerra de redes entonces emplea y se desarrolla en dos escenarios, a saber: la realidad, con las actividades diarias que realizan los individuos de cada una de las células de la organización, y lainternet, como una constante lucha de obtención de información (Arquilla y Zanini, 2001: 14).

En consecuencia, la obtención de información de seguridad nacional es una situación que pondría a los Estados en un punto crítico, debido a su dependencia de los sistemas informáticos. Esto, porque con la información necesaria se pueden planear operaciones que alteren el orden público de un país, y la búsqueda de información de los grupos terroristas se basa en buscar los puntos débiles de los Estados; aunque este último sería el objetivo final, las organizaciones terroristas también emplean internet y demás tecnologías de la información y la comunicación para realizar actividades propagandísticas y de reclutamiento, con el fin de informar o transmitir un mensaje ideológico (González, 2002: 17).

A propósito de ese nuevo fenómeno de la organización en redes de los grupos terroristas, Arquila y Ronfeldt (2001: 49) proponen la creación de redes dentro de las fuerzas armadas y los entes gubernamentales. Estos dos autores definen esta nueva doctrina como "enjambre", es decir, la creación de una red de fuerzas altamente especializadas y con gran capacidad de despliegue y fuego en el momento y el lugar adecuados.

Enjambre es una red que integra diferentes grupos que poseen la capacidad de interconectarse entre sí para entablar comunicación y unirse rápidamente en torno a algún objetivo específico y, posteriormente, volver a dispersarse. Implementar este mismo sistema en sistemas defensivos resultaría bastante útil, debido a que sería difícil de descifrar una red en términos de organización. Un enemigo no tendría un plano sobre la actuación de los mecanismos de defensa, los actores que entrarían en acción, en dónde apoyarían y cómo actuarían (Arquilla y Zanini, 2001: 15).

Por tanto, las redes para Arquila y Ronfeldt son la transformación de los grupos que anteriormente permanecían bajo una estructuración jerárquica que dificultaba sus ejecuciones terroristas. Ahora las redes –que empiezan a tornarse más fuertes, difíciles de desarticular y difíciles de localizar– permiten a las organizaciones terroristas romper el esquema jerárquico para emplear técnicas asimétricas aplicadas a las nuevas tecnologías de la información y ampliar las fronteras del campo de batalla.

Teniendo en cuenta todo lo anterior, se deduce que las nuevas tecnologías han dado paso a una novedosa forma de expresión del terrorismo, conocida como ciberterrorismo, que en primera instancia hace referencia a todas las actividades que ejecutan las organizaciones terroristas, haciendo uso de las tecnologías de la información y la comunicación, ya sea afección a la infraestructura crítica, robo de información de seguridad nacional, propaganda o reclutamiento.

Barry Collin, un investigador del *Institute for Security and Intelligence* de California, acuñó el término ***cyberterrorism*** para referirse a "la convergencia del ciberespacio con el terrorismo" (1997: 13). Mark Pollit, agente del FBI que se dedicó a estudiar el tema, desarrolló la siguiente definición operativa: "El ciberterrorismo es el ataque premeditado y políticamente motivado contra información, sistemas computacionales, programas de computadoras y datos que puedan resultar en violencia contra objetivos no combatientes de grupos subnacionales o agentes clandestinos" (Masana, 2002: 12).

El terrorismo antes de las tecnologías de la información y la comunicación

El terrorismo es un medio que se ha utilizado a lo largo de la historia para conseguir fines, en su mayoría políticos. Busca persuadir a un gobierno de la manera más drástica, es decir, mediante acciones violentas e indiscriminadas contra la población, generando conmoción y desorden dentro del Estado con el fin de que este cambie sus políticas o centre su atención en lo que buscan estos grupos (Virginia, 2002: 11).

Walter Laqueur (1997) dice en su libro *Una historia del terrorismo* que "a lo largo de los siglos, el terrorismo se ha presentado bajo muchas apariencias, sus motivos, sus metas y su modus operandi" (p. 7). En tal sentido, las manifestaciones del terrorismo se remontan a los siglos XI y XII;en aquel entonces, la secta musulmana radical shiíta de "Los asesinos" aterrorizaba Persia por medio de actos suicidas en contra de personalidades políticas (Pizarro, 2002, párr. 8).

De esta manera, antes de que los grupos terroristas tuvieran acceso a las tecnologías de la información y la comunicación para cumplir sus metas, estos se configuraban bajo una organización jerárquica que los hacía netamente regionales y más vulnerables a las acciones militares. En ese contexto, carente de las tecnologías actuales, los grupos terroristas tenían como objetivos principales lo siguiente:

1. Intimidar o ejercer coerción sobre la población civil.
2. Influir en la política de un gobierno por medio de la intimidación o la coerción.
3. Afectar la conducta de un gobierno por medio del asesinato o el secuestro. (Mercado y Olvera, 2009: 129).

Una vez mencionados los propósitos centrales del terrorismo es necesario describir sus principales características, definidas por Miguel Cano (2009) de la siguiente manera:

> Una característica común a este tipo de organizaciones terroristas tradicionales es que las acciones las llevaban a cabo exclusivamente dentro del territorio, dentro de su propio Estado. Además, los actos terroristas de estas organizaciones de corte "clásico" tenían un marcado carácter selectivo, dirigiéndose fundamentalmente contra determinados individuos o instituciones representantes del poder opresor que trataban de combatir. (p. 22)

Así, el terrorismo constituía simplemente una herramienta para ir en contra de las políticas de un Estado o de un sector privado dentro de sus propias fronteras, sin alterar el orden de los actores del sistema internacional y afectando solamente a una nación, para suplir las necesidades de un determinado grupo terrorista. En consecuencia, cada uno de los grupos terroristas se alinea bajo intereses que los identifican respecto a los demás grupos de la sociedad. Según Cano (2009):

> Fue principalmente a comienzos de la década de 1970 cuando de un modo paulatino aparecieron en determinados países europeos una serie de grupos u organizaciones, los cuales pretendían mediante la ejecución de acciones terroristas, bien sustituir un determinado sistema político-social por otro más acorde con sus postulados ideológicos (terrorismo de carácter social-revolucionario, representado en su momento por organizaciones terroristas como la RAF en Alemania o las Brigadas Rojas en Italia), bien lograr la escisión total o parcial de un determinado territorio de la soberanía ejercida por un Estado (terrorismo de carácter etnonacionalista, como fue el caso del IRA en Irlanda del Norte, o sigue siendo el caso de ETA en España). (p. 2)

Dentro de las tácticas más comunes diseñadas por los grupos terroristas se encuentra un determinado listado de acciones que eran planeadas desde un punto de reunión predeterminado en el que se establecían los parámetros para la ejecución de sus actos. Todo debía ser detalladamente planeado debido a las limitaciones de comunicación que enfrentaban durante la ejecución de su actividad, desde quiénes serían los autores, qué función cumpliría cada uno de sus integrantes y en qué momento actuarían.

La selección de blancos ha sido lo más importante a la hora de la realización de sus atentados porque son clasificados como simbólicos o pragmáticos; para ellos lo más importante es lograr mayor poder de atención para difundir su mensaje y proyectar su influencia sobre el público. Por tanto, no lograr la atención de los medios podría ser la mayor limitación para su interés, por lo que se reitera que antes de las actuales tecnologías los grupos terroristas eran netamente regionales (Escuela de las Américas, 1989: 8). En consecuencia, la definición de objetivos de los grupos terroristas recae sobre los más simbólicos, dado que transmiten fácilmente el mensaje terrorista a la sociedad: el Estado es incapaz de proteger a la ciudadanía, generando así un ambiente de temor e inseguridad (Escuela de las Américas, 1989: 9). Es notable que todas estas actividades sean realizadas por un mismo Estado, pues las tecnologías de la información y la comunicación que prevalecían anteriormente no tenían la fuerza suficiente para llevar el mensaje por fuera de las fronteras nacionales (Masana, 2002: 38).

Hacia una conceptualización del ciberterrorismo

Desde la década de 1980 el surgimiento y la proliferación de nuevas tecnologías han traído grandes cambios en la forma de organización de la sociedad, desde lo más básico hasta lo más complejo; desde realizar una simple compra en cualquier tienda hasta formalizar grandes negocios a escala mundial. El terrorismo no escapa a esta lógica de la globalización. Por tal motivo, este capítulo está enfocado a dar a conocer las razones por las cuales el ciberterrorismo es una amenaza para los Estados del sistema internacional, con fundamento en que este problema ha adquirido la capacidad de influenciar la tecnología de la comunicación y la información con el fin de facilitar el desarrollo de sus actividades (Botta, 2005: 6).

El ciberterrorismo ha sido la evolución del terrorismo que, aprovechando el desarrollo tecnológico de la misma sociedad, ha encontrado nuevos campos desde dónde actuar y causar mayor daño aun a un Estado que no tuviese la

capacidad informática de protegerse (Cano, 2008: 4). El ciberterrorismo le da distintos usos a internet: como objeto de ataque en el que un objetivo rentable sería la infraestructura crítica de un Estado, como instalaciones, redes, servicios, equipos físicos y de tecnología de la información cuya inutilización tendría un impacto mayor en la seguridad de los ciudadanos y el eficaz funcionamiento de los gobiernos (Guardia Civil de España, 2008: 12).

En este contexto, el ciberterorismo se ha venido evidenciado como una amenaza y por tanto ya algunos países han creado dentro de sus fuerzas armadas unidades especiales con el fin de desempeñarse en el campo de la ciberdefensa (Andress y Winterfeld, 2011: 199). La principal misión de estas unidades es desarrollar las capacidades de defensa y ataque contra organizaciones terroristas mediante el uso de la tecnología para neutralizar sus labores y mantener la seguridad de los Estados (Torres, 2011: 14).

Las nuevas tecnologías permiten a los grupos terroristas romper todos los esquemas del antiguo terrorismo, lo que da lugar a la aparición del ciberterrorismo como un nuevo fenómeno con capacidades y herramientas que facilitan el desarrollo de sus actividades. La evolución del terrorismo al ciberterrorismo implica pasar de acciones basadas en artefactos explosivos, hostigamientos y movimiento de hombres, hacia acciones realizadas por una sola persona con un dispositivo electrónico conectado a internet desde cualquier parte del mundo, con capacidad para amenazar la seguridad nacional de cualquier Estado. En tal sentido, existen nuevas tácticas empleadas por las organizaciones terroristas que se basan esencialmente en el uso de las nuevas tecnologías. De esta manera es posible evidenciar cómo la implementación de estas herramientas dio un giro rotundo a la naturaleza de los conflictos (Arquilla y Zanini, 2001: 13).

Un ejemplo de lo anterior es el uso de las nuevas tecnologías para obtener información que facilite labores de inteligencia y mejore el planeamiento sobre determinados blancos considerados de alto valor para las organizaciones terroristas. Para el efecto, se hace uso de herramientas muy comunes hoy en día como *Google Earth* y *Google Maps*, con las que se pueden generar mapas en ciudades importantes para ubicar bombas, tener puntos de reunión, rutas de escape y facilitar la ejecución de acciones terroristas físicas. Todo esto lo puede ejecutar, desde cualquier parte del mundo, una sola persona que después distribuirá la información en su red para el planeamiento de un ataque.

Por otro lado, el ciberterrorismo ofrece ventajas de seguridad al terrorista, porque no se expone físicamente y puede permanecer en el anonimato,

actuando desde cualquier parte del mundo. En este sentido, como lo expone la Guardia Civil de España (2008), un ciberataque puede ser ejecutado por una sola persona, puede crear mayor conmoción que un ataque tradicional y es más económico (p. 18).

Como resultado, la principal dificultad para un Estado ante un ciberataque es identificar de dónde provino el ataque y quién es el atacante, debido a que los ciberataques no dejan rastros fácilmente identificables. En respuesta, el Estado agredido puede poner en marcha la activación de sus sistemas de ciberdefensa solamente para frenar el ataque, pero no para llegar hasta la posición de su enemigo para neutralizarlo. Es más complicado aún si el atacante no fuera solo uno, sino varios ordenadores desde cualquier parte del planeta (Torres, 2011: 14).

Para comprender lo anterior, se deben identificar las distintas maneras de ejecutar un ciberataque. Estas son: alojando archivos dañinos directamente en los servidores del ente objetivo, esto sucede cuando el ente objetivo no conoce todas sus debilidades informáticas y deja brechas abiertas para la filtración de agentes externos a su sistema (Lejaraza, 2014: 9). Otra manera es infectando diferentes ordenadores conectados a internet, por medio de una página web que albergue algún tipo de archivo dañino, que se descargará automáticamente una vez sea visitada la página web en la quese aloja. En muchas ocasiones los usuarios no se darán cuenta. Este archivo está programado de tal manera que a la llegada de determinada fecha y hora todos los ordenadores infectados enviarán automáticamente miles de mensajes al ente objetivo saturando sus sistemas, lo que configura un ataque de denegación de servicio (Garzón, 2013: 19).

Ante la facilidad relativa de los ciberataques, los terroristas han descubierto que las naciones industrializadas son más débiles en el ciberespacio, porque estos países han hecho de la tecnología la forma de vida del siglo XXI y se han vuelto prácticamente dependientes de ella. Aunque en primera instancia el ciberterrorismo no cause daño físico a la población, sí genera cierta alteración psicológica debido a que ataca a las instituciones que predominan en ella, dejándola vulnerable y por consiguiente causando desconfianza hacia ellas, al no ser capaces de proteger contra estos ataques (Hernangómez, 2014: 3).

En consecuencia, el ciberterrorismo, como la nueva expresión del fenómeno del terrorismo en el siglo XXI, constituye todo lo que las organizaciones terroristas pueden hacer a un costo menor en cuanto a esfuerzo, seguridad y economía, con el propósito de conseguir mejores resultados, haciendo que su ideología se expanda no solo dentro de lasfronteras nacionales, sino que genere repercusiones en el sistema internacional (Lewis, 2002: 7).

Actividades ciberterroristas en internet

Se entiende por ciberterrorismo todas las actividades realizadas por organizaciones terroristas que comprometen el uso de las tecnologías de la información y la comunicación, ya sea en sus actividades de carácter propagandístico, reclutamiento, información, recaudación de fondos, comunicación, entrenamiento o ciberataques que tienen como finalidad hurtar información para la realización de atentados contra las infraestructuras informáticas de los Estados o sectores privados de la sociedad (Díaz, 2010: 231).

En esta dinámica, desde 1998, Dale Watson, jefe de la Sección de Terrorismo Internacional del FBI, aseguró que los grupos terroristas estaban iniciando una carrera en el uso de las nuevas tecnologías de la información y la comunicación para informar y reclutar nuevos miembros. Pero fue hasta el 11 de septiembre de 2001 cuando los estados prestaron atención a este informe. Después de dicha fecha todas las páginas relacionadas con temas terroristas –que contenían desde instrucciones de cómo recaudar fondos, hasta cómo fabricar bombas caseras– empezaron a ser clausuradas (Merlos, 2006: 89).

Por ejemplo, compañías como Yahoo, la sección europea del buscador Lycos.com y la página de Azzam.com se sometieron a la búsqueda de páginas y enlaces que difundieran cualquier contenido relacionado con el terrorismo y procedieron a eliminarlas. Aunque debido a la existencia de un gran número de servidores, estas organizaciones terroristas siguen buscando y encontrando la forma de difundir su mensaje (Masana, 2002: 40). Al respecto, en internet se encuentran páginas web de distintos grupos terroristas, desde las que difunden su ideología por medio de mensajes e informando lo que sucede o hacen dentro de la organización.

Otro ejemplo es el movimiento de resistencia islámica *Hamas,* quetiene la siguiente dirección http://www.hamasinfo.net/ por medio de la cual dan a conocer constantemente las actividades más recientes realizadas por sus integrantes, rinden tributo a quienes en actos de terrorismo han perdido la vida o están presos, publican fotografías de líderes y de las actividades que realizan, hacen invitaciones a continuar en su lucha, entre otras actividades (Sánchez, 2010b: 204.). Así mismo, se encuentra una página del *Hezbollah,* en la siguiente dirección http://www.moqawama.org/ en la que se pueden encontrar vínculos que divulgan noticias sobre la organización y todo lo que gira en torno a ella, como actividades de otros Estados y organizaciones; también hay archivos de audio, fotos, biografías, informes de guerra y una sección especial para contactar con la organización (Sánchez, 2010b: 204).

En otra ubicación geográfica, en Colombia, se encuentra el grupo insurgente más antiguo del mundo: las Fuerzas Armadas Revolucionarias de Colombia FARC,que administran la página webwww.farc-ep.codesde la cual informan sobre "partes de guerra" y detallan cada uno de los combates que desarrollan contra el Ejercito de Colombia. Allí, tienen una sección especial en la quese escribe para soldados y policías del país y publican sus comunicados. La página está disponible en inglés y en francés. También se apoyan en páginas subsidiarias como Anncol, en laque publican noticias críticas al Gobierno e información proclive a sus intereses. (Bermúdez, 2011: 109).

De la misma manera, el Ejército de Liberación Nacional (Eln) dispone de la dirección www.eln-voces.commediante, en la cual se identifican, dan a conocer su escudo, su himno y su bandera. La página web también está traducida en varios idiomas y cuenta con una sección para establecer contacto con ellos, informan lo que sucede y publican videos en la plataforma youtube.com.

Es evidente el uso prioritario que las organizaciones terroristas han dado a internet como medio de comunicación masivo para mantener el contacto con todos sus integrantes y difundir un mensaje que pueda sobrepasar las fronteras del Estado donde normalmentedesarrolla sus actividades. Al realizar una comparación de cada una de las páginas de estos grupos terroristas, es fácil identificar su necesidad de emitir mensajes familiarizados fuertemente con sus ideologías. Al tiempo invitan a la violencia, resaltan sus actividades militares y martirizan a sus líderes muertos.

La organización separatista vasca ETA intentó sostener también una página web para difundir propaganda e intereses de la organización, pero sus propósitos cibernéticos fueron obstaculizados por cibernautas españoles que consiguieron saturar en muchas ocasiones consobrecarga de mensajes los servidores en los que se montaba la página, haciendo que esta quedara fuera de funcionamiento, como en el caso del proveedor Institute for Global Communication (IGC) y del periódico vasco ***Gara,*** en el que ETA realizaba publicaciones o asumía responsabilidades de ataques perpetrados. ETA no ha sido tan contundente en el uso de internet debido a que activistas cibernéticos siempre se han propuesto la tarea de impedir que divulguen sus pronunciamientos ideológicos por medio de una página web propia y las que han sido usadas como medio de comunicación también han sido atacadas (Masana, 2002: 35).

Lo mismo sucedió con la organización terrorista Al-Qaeda el 6 de junio de 2011, con la publicación de su revista ***Inspire*** en la web, en la que ofrecían entrenamiento sobre cómo preparar bombas, cómo utilizar un AK-47, cómo

explotar un edifico con gas natural, entre otros temas. Esta fue hackeada por el servicio de inteligencia británico MI6 que la modificó y cambió los manuales de información terrorista por recetas para preparar ponqués (Thomas, 2003: 112).

Conclusiones

Las tecnologías de la información y la comunicación transformaron todas las actividades humanas, incluyendo la guerra, en lo que se ha conocido como la era de la información, en las que los modelos operativos han adoptado el concepto de red como paradigma de funcionamiento, han generado procesos más flexibles, adaptables, descentralizados y complejos en la economía, el comercio, la diplomacia y la seguridad internacional.

A la luz de esta tendencia, las organizaciones terroristas han intensificado el uso de las nuevas tecnologías, lo que les ha permitido descentralizar sus actividades, coordinar mejor sus actuaciones en el mundo real, acceder a información de seguridad nacional y atacar la infraestructura critica de los Estados. A su vez, las nuevas tecnologías han transformado los modelos operativos de las organizaciones terroristas, esto da origen al concepto de guerra en red, porque estas organizaciones, al ser más flexibles y descentralizadas, aumentan su capacidad de hacer daño a la sociedad y, al mismo tiempo, el grado de amenaza que representan para los Estados y para el sistema internacional. En tal sentido, la guerra en red se convierte en un modelo que las fuerzas de seguridad de los Estados deben comprender en aras de diseñar mejores estrategias contra el ciberterrorismo.

Como respuesta, los Estados deben implementar procesos más descentralizados y flexibles en sus fuerzas de seguridad, para que puedan dar una respuesta proporcional a la amenaza que supone el ciberterrorismo; deben realizar procesos interagenciales más complejos, para que múltiples instituciones puedan integrar esfuerzos con el propósito de neutralizar el terrorismo y el ciberterrorismo. Igualmente, es necesario incentivar una evolución organizativa en los organismos de seguridad, tendiente a flexibilizar las estructuras jerárquicas, lo que favorecerá una operación antiterrorista más rápida y eficiente, en coherencia con el modelo de guerra en enjambre que se propone en respuesta a la guerra en red de las organizaciones terroristas en la era de la información.

Desde esta perspectiva, el ciberterrorismo es cualquier actividad que las organizaciones terroristas ejecuten en internet o con apoyo de las tecnologías de la información y la comunicación. Esto implica una gran diversidad de

acciones, que no se restringe al robo de información de seguridad nacional o al ataque a infraestructura crítica de los Estados conectada a la red, sino que se amplía a la divulgación de información ideológica, coordinación de actos terroristas, reclutamiento, propaganda, entre otras. Así, queda en evidencia la importancia que tiene para los grupos terroristas la implementación de las tecnologías de la información y la comunicación dentro de sus organizaciones, permitiéndoles sus frentes de acción más allá de las fronteras de los Estados en los que normalmente operan. En tal sentido, las tecnologías de la información han ampliado el rango de acción del terrorismo y les han otorgado una nueva posición como actores dentro del sistema internacional, principalmente como representantes de la nueva amenaza del ciberterrorismo.

Desde este punto de vista, la coordinación y cooperación entre los Estados es un requisito ineludible para neutralizar el terrorismo en la era de la información, en la medida en que este puede trascender más fácilmente las fronteras nacionales como resultado del uso sistemático de las nuevas tecnologías. Por ello, con marcos de cooperación internacional tendientes a neutralizar las actividades terroristas en internet, incluyendo capacitación en ciberdefensa y ciberseguridad, los Estados podrán afrontar de una mejor manera la nueva amenaza del ciberterrorismo.

Referencias

1. Andress, J. y Winterfeld, S. (2011). *Cyber Warfare: Techniques, Tactics and Tools for Security Practitioners*. Washington: Waltham Syng Press.
2. Arquilla, J. y Ronfeldt, D. (1996). *The Advent of Netwar*. California: RAND Corp.
3. Arquilla, J. y Zanini, D. (2001). *Redes, guerra en red y era de la información*. Madrid: Alianza Editorial.
4. Arquilla, J. y Zanini, D. (2001). *Networks and Netwars*. California: RAND Corp.
5. Arquilla, J. y Zanini, D. (1997). *Cyber War is Coming*. California: RAND Corp.
6. Arquilla, J. y Zanini, D. (2001b). *Guerra en red y era de la información*. California: RAND Corp.
7. Bermúdez, L. (2011). Ciberterrorismo: el lado oscuro de la red. Revista *Academia Libre*. Año 8, No. 9. Recuperado de http://www.unilibrebaq.edu.co/unilibrebaq-test/revistas2/index.php/academialibre/article/download/263/236
8. Brenner, S. (1999). *Cyberthreats: The emerging Fault Lines of the Nation State*. New York: Oxford University Press.
9. Botta, J. (2005). *El uso de internet por parte de los grupos terroristas yihadistas*. Documento de Análisis No. 4, Centro Argentino de Estudios Internacionales. Recuperado de http://www.caei.com.ar/sites/default/files/04.pdf
10. Cano, J. (2008). Ciberseguridad y ciberdefensa: dos tendencias emergentes en un contexto global. Revista *Sistemas*. No. 119.Recuperado de https://www.acis.org.co/fileadmin/Revista_119/Editorial.pdf
11. Cano, M. (2009). Reflexiones en torno al viejo y al nuevo terrorismo. Revista *Española de Investigación Criminológica*. Artículo 7, No. 7. Recuperado de http://www.criminologia.net/pdf/reic/ano7-2009/a72009art7.pdf
12. Castells, M. (2001). *La galaxia internet: reflexiones sobre internet, empresa y sociedad*. Madrid: Plaza y Janes Editores.
13. Castells, M. (1999). *La era de la información: economía, sociedad y cultura*.Vol. 1. Ciudad de México: SigloXXI Editores.
14. Collin, B. (1997).*The Future of CyberTerrorism: Where the Physical and Virtual Worlds Converge*. 11th Annual International Symposium on Criminal Justice Issues. California: Institute for Security and Intelligence.
15. Denning, D. (2001). *Activism, Hacktivism, and Cyberterrorism: the Internet as a tool for influencing foreign policy*. California: RAND Corp. Recuperado de http://www.rand.org/content/dam/rand/pubs/monograph_reports/MR1382/MR1382.ch8.pdf
16. Díaz, J. (2010). La ciberseguridad en el ámbito militar. En Ciberseguridad, retos y amenazas a la seguridad nacional en el ciberespacio. *Cuadernos de Estrategia*. No. 149. Instituto Español de Estudios Estratégicos. Recuperado de http://bibliotecavirtualdefensa.es/BVMDefensa/i18n/catalogo_imagenes/grupo.cmd?path=17029
17. Escuela de las Américas. (1989). *Manual de terrorismo y guerrilla urbana*. Instituto del Cusseta, GA, Estados Unidos: Hemisferio Occidental para la Cooperación en Seguridad. Recuperado de http://derechos.org/nizkor/la/libros/soaGU/index.html
18. Garzón, R. (2013). Ciberguerra, temor, incertidumbre y duda. *Information Security and Risk Managment Conference*, Sesión 133. Recuperado de http://www.isaca.org/Education/Conferences/Documents/Latin-CACS-2013-Presentations/133.pdf
19. González, I. (2002). Ciberterrorismo: una aproximación a su tipificación como conducta delictiva. Revista *Pensamiento Penal* No. 22. Recuperado de http://www.dialnet.unirioja.es/descarga/articulo/3311844

20. Guardia Civil de España. (2008). *El uso de internet por organizaciones terroristas*. Madrid, España. Recuperado de http://scm.oas.org/pdfs/2008/CICTE00341T.pdf
21. Hernangómez, J. (2014). Dilemas cibernéticos y la estrategia de seguridad nacional. *Documentos de Opinión*. No. 6. Madrid, España: Instituto Español de Estudios Estratégicos. Recuperado de http://www.ieee.es/Galerias/fichero/docs_opinion/2014/DIEEEO06-2014_DilemasCiberneticos_JL.Hernangomez.pdf
22. Laqueur, W. (1999). *The New Terrorism*. New York: Oxford University Press.
23. Laqueur, W. (1997). *Una historia del terrorismo*. Madrid, España: Paidós Ibérica.
24. Lewis, J. (2002). *Assessing the Risks of Cyberterrorism, Cyber War and Other Cyber Threats*. Washington: Center for Strategic and International Studies. Recuperado de http://csis.org/publication/assessing-risks-cyber-terrorism-cyber-war-and-other-cyber-threats
25. Lejaraza, E. (2014). Ciberguerra, los escenarios de confrontación. *Documento de Opinión*. No. 18. Madrid, España: Instituto Español de Estudios Estratégicos. Recuperado de http://www.ieee.es/Galerias/fichero/docs_opinion/2014/DIEEEO18-2014_Ciberguerra_EscenariosConfrontacion_EguskineLejarza.pdf
26. Masana, S. (2002). *Ciberterrorismo: ¿una amenaza para la paz mundial?* San José, Costa Rica: Facultad Latinoamericana de Ciencias Sociales. Recuperado de http://www.argentina-rree.com/documentos/ciberterrorismo.pdf
27. Mercado, A. y Olvera, G. (2009). La crisis del orden mundial: globalización y terrorismo. Revista *Relaciones Internacionales, Estrategia y Seguridad*. Vol. 4, No. 1. Recuperado de http://www.umng.edu.co/documents/63968/76559/8--Dr.AsaelMercadoyotros.pdf
28. Merlos, A. (2006). Internet como instrumento para la yihad. *Araucaria. Revista Iberoamericana de Filosofía, Política y Humanidades*. No. 16. Sevilla, España.Recuperado de http://www.dialnet.unirioja.es/descarga/articulo/2098457
29. Pizarro, E. (23 de diciembre, 2002). Viejo y nuevo terrorismo. Revista *Semana*. Recuperado de http://www.semana.com/mundo/articulo/viejo-nuevo-terrorismo/55660-3
30. Sánchez, G. (2010). Internet: una herramienta para las guerras del siglo XXI. *Military Review en Español*, Julio-agosto. Fort Leavenworth, KS. Recuperado de http://usacac.army.mil/CAC2/MilitaryReview/Archives/Spanish/MilitaryReview_20100831_art006SPA.pdf
31. Sánchez, G. (2010b). La nueva estrategia comunicativa de los grupos terroristas. Revista *Enfoques, Ciencia Política y Administración Pública*. Vol. VIII, No. 12. Recuperado de http://www.ucentral.cl/prontus_ucentral2012/site/artic/20131231/asocfile/20131231215635/20101210.pdf
32. Torres, M. (2011). Los dilemas estratégicos frente a la ciberguerra. *Revista del Ejército español*. No. 839. Recuperado de http://www.upo.es/personal/mrtorsor/Publicaciones.html
33. Torres, M. (2009). Terrorismo yihadista y nuevos usos de internet: la distribución de propaganda. *ARI* No. 110. Madrid, España: Real Instituto Elcano. Recuperado de http://www.realinstitutoelcano.org/wps/portal/rielcano/contenido?WCM_GLOBAL_CONTEXT=/elcano/elcano_es/zonas_es/terrorismo+internacional/ari110-2009
34. United Nations Office on Drugs and Crime (UNODC) (2013). *El uso de internet con fines terroristas*. Organización de Naciones Unidas. Recuperado dehttp://www.unodc.org/documents/terrorism/Publications/Use_of_Internet_for_Terrorist_Purposes/Use_of_Internet_Ebook_SPANISH_for_web.pdf
35. Virginia, M. (2002). *El espíritu del terrorismo*. París: Galilée.