Ciberterrorismo en el ciberespacio como actuación alternativa del terrorismo tradicional

Cyberterrorism in cyberspace as an alternative action to traditional terrorism

Capitán de Fragata CJ Angelita del Rosario Huapaya Rueda. Segundo Comandante de la Comandancia de Ciberdefensa de la Marina de Guerra del Perú. Abogada de profesión y magíster en Derecho por la Pontificia Universidad Católica del Perú. Ostenta el máster en Seguridad y Defensa por la Universidad Nebrija (España). Fue discente en el Primer Curso de Asesores Jurídico-Operacionales organizado por el Comando Conjunto de las Fuerzas Armadas y el Ministerio de Defensa. Asimismo, estudió en el Centro de Derecho Internacional Humanitario y Derechos Humanos (Perú), y en el Instituto Internacional de Derecho Humanitario en San Remo (Italia). Siguió el curso de Estado Mayor en Operaciones de Paz en la Escuela de Misiones Internacionales y Acción Integral (ESMAI, Colombia). Es docente en Derecho Internacional de los Derechos Humanos en la Marina de Guerra del Perú, y en Derecho Internacional Humanitario en el Centro de Entrenamiento y Capacitación para Operaciones de Paz (CECOPAZ).

Resumen: Hoy en día, se concibe al ciberespacio como un nuevo ámbito de los conflictos armados, y donde, también, podemos encontrar crimen organizado, espionaje y, por supuesto, grupos terroristas. Este espacio transversal está siendo utilizado para facilitar al atacante la posibilidad de actuar de forma anónima, creando, a su vez, ciberarmas, como el *malware*, el cual, por el momento, es considerada un arma de disrupción masiva, pero con probabilidades de convertirse en un arma de destrucción masiva que pueda afectar infraestructuras críticas de un Estado. El presente artículo busca enfocar cómo el terrorismo se ha repotenciado con el uso creciente de las tecnologías de información y comunicaciones (TIC) y del Internet, que pueden afectar a sectores del Estado susceptibles de sufrir ciberataques masivos, y provocar graves daños económicos, sanitarios y de índole moral a la población a través de sus vulnerabilidades, especialmente las del "día cero",[1] las cuales son vendidas y explotadas por los ciberterroristas.

1 También, conocido como "exploits de día cero", son aquellos ataques realizados por ciberdelincuentes, cuyo objetivo es buscar, encontrar y aprovechar las vulnerabilidades existentes, conocidas previamente y desconocidas en el *software*.

Palabras clave: Ciberespacio, ciberterrorismo, *malware, hackers*, propaganda, difusión, terror.

Abstract: *Nowadays, cyberspace is conceived as a new sphere of armed conflicts, where we can also find organized crime, espionage and, of course, terrorist groups. This transversal space is being used to facilitate the attacker the possibility of acting anonymously, creating in turn cyberweapons such as malware, which for the moment is considered a weapon of mass disruption, but which will probably become a weapon of mass destruction that can affect critical infrastructures of a state. This article seeks to focus on how terrorism has been enhanced by the growing use of Information and Communication Technologies (ICTs) and the Internet, affecting the sectors of the state, which are susceptible to massive cyber-attacks, and can cause serious economic, health and moral damage to the population, through its vulnerabilities, especially those of "zero day", which are sold and exploited by cyber-terrorists.*

Keywords: *Cyberspace, cyberterrorism, malware, hackers, advertising, diffusion, terror.*

El fin del terrorismo no solo es causar caos, destrucción o muerte, también, es enviar un mensaje de odio para desestabilizar al enemigo, y ahora, además, lo hace a través y mediante el ciberespacio.

Terrorismo tradicional

Consideraciones generales

El terrorismo tradicional es concebido como aquel acto destinado a causar muerte o lesiones corporales a las personas con un determinado propósito, ya sea económico, social, religioso o político; asimismo, se ha podido comprobar, a lo largo de la historia y en muchos lugares del mundo, que este tipo de actuación se ha venido realizando en menor o mayor medida, pero utilizando siempre el terror como símbolo de presentación, y en diferentes formas, unas más crueles que otras, pero sin dejar de causar daños irreparables.

A nivel mundial, entre las organizaciones terroristas más conocidas que han alcanzado cierta notoriedad se encuentran las siguientes:

a. Talibán
b. Estado Islámico
c. Al-Shabaab
d. Maoístas
e. Al-Qaeda
f. Houthi extremists
g. National Liberation Army of Colombia
h. Janjaweed
i. Democratic Front for the Liberation of Rwanda
j. Seleka. (Pérez, 2015, p. 69)

Para efectos del presente artículo, nos avocaremos a citar a los grupos yihadistas.

Objetivos de los grupos terroristas

Tomemos como ejemplo, según lo definido por Pérez, los objetivos autoimpuestos por uno de los grupos terroristas yihadistas denominado Estado Islámico:

a. A corto plazo: buscar consolidar el territorio que tiene controlado, y, en la medida de lo posible, ampliarlo. Tal es así que ha utilizado como táctica en Irak, la confrontación entre sunnís y chiitas.
b. A mediano plazo: buscar continuar ampliar su dominio, para lo cual pretende extender el mismo a los países dominados o controlados por los sunnitas.
c. A largo plazo: buscar crear un único Estado musulmán y, de ser posible, la dominación mundial. (2015, p. 101)

Cabe mencionar que, según reportes periodísticos, en el 2021, los países que han sufrido más atentados terroristas de ideología yihadista han sido: Afganistán, Burkina Faso y Malí. El terrorismo yihadista ha sido el más cruel y al que se le atribuye la mayor cantidad de muertes en el mundo.

Una mirada hacia el terror

Para González Calleja y Rapoport, existen cinco oleadas del terrorismo, las cuales podemos conceptuar como cinco actuaciones concretas para conocer cómo actúa el terrorismo moderno. Las tres primeras oleadas son

como siguen: primera, la "anarquista"; segunda, la "anticolonial"; y tercera, la "yihad mayor", que es la lucha dentro de uno mismo, su lucha interior. La cuarta oleada consiste en los atentados suicidas, empleados como una innovación táctica; bajo esta forma de impartir terror, se han perpetrado numerosos atentados contra instalaciones gubernamentales y militares extranjeras, especialmente estadounidenses (Rapoport, 2004). Asimismo, González señala como quinta oleada a la religión. Los terroristas utilizan la religión para justificar su accionar, cuyo objetivo es "cumplir un mandato divino o imponer a otros por la fuerza una determinada visión trascendente de la vida" (2012, p. 53).

En todas estas oleadas, se han utilizado métodos extremos, sufrimientos físicos, inhumanos, crueles y degradantes, con los cuales los terroristas se hacen conocer ante los medios de comunicación para sembrar el terror y buscar debilitar a su oponente.

Ciberterrorismo. Actividades terroristas en el ciberespacio

Un enfoque distinto, pero el mismo terror

Coincidimos con lo expuesto por Cárdenas al señalar que, será considerado como ciberterrorismo todas aquellas actividades realizadas por terroristas mediante la utilización de las TIC, como, por ejemplo, propagandas, reclutamientos o ciberataques, y cuyo propósito sea atentar contra las infraestructuras informativas de los Estados o sectores privados (2022, p. 1). El terror mediante el ciberespacio se ha convertido en una real pesadilla para todas las naciones y en particular en Occidente. Esta nueva visión del terror y, sobre todo, del terrorismo yihadista, ha generado sus propias características destructivas en el ciberespacio.

Conforme avanzan las TIC también progresan las amenazas de los ciberterroristas en todo el mundo, y, de concretarse, estas pueden ser tan o más destructivas que las amenazas en el mundo físico; por ello, se necesita contar con expertos, nuevas tecnologías y con un marco legal apropiado para sancionar a estos grupos terroristas.

¿Cómo actúan los ciberterroristas en el ciberespacio?

Los ciberterroristas actúan en tres aspectos:

a. Propaganda. Los terroristas buscan convertirse en el centro de la atracción utilizando la propaganda y la publicidad. Con las TIC, la propaganda se ha vuelto más eficiente y su forma de propagación es tan rápida que genera un atractivo significativo para los grupos terroristas, cuyo objetivo es hacer llegar su mensaje en todo el mundo. Como bien señala Cárdenas, la propaganda que usan los grupos terroristas será aquella que, de una u otra manera, pueda perjudicar la protección de la seguridad nacional o que incite a la comisión de actos de violencia contra personas o grupos específicos (2022, p. 4).

b. Reclutamiento. Al igual que en el mundo real, los grupos terroristas buscan cambiar mentes, adoctrinar gente, contribuir a su causa, utilizando medios virtuales; de esta forma, las personas se adhieren a ciertas ideas, por lo general radicales, que las pueden conducir a cometer actos terroristas.

c. Adoctrinamiento. Reclutan a sus miembros previo proceso de adoctrinamiento, mediante el cual consiguen plasmar una ideología en sus seguidores, quienes están convencidos de seguirla. Una vez adheridos a determinado grupo, los conducirán a cometer actos terroristas, cuya ideología radical favorece la conflictividad con otros grupos y el empleo de la violencia.

Es importante mencionar la recaudación o financiación terrorista, consideradas como actividades propias del ciberterrorismo, las cuales consisten en apoyar financieramente los actos de estos grupos, ya sea suministrando fondos, bienes u otros recursos.

Por ejemplo, en el 2005, en el Reino Unido, se detectó el robo de tarjetas de crédito para financiar actos terroristas. Fueron creados varios sitios web y foros para incitar al terrorismo, como al homicidio en Iraq. Asimismo, en el 2020 fueron detenidas treinta personas por ciberfinanciación terrorista, al haber, supuestamente, transferido dinero a miembros de ISIS y de Al Qaeda en Siria. Otra forma fue realizar una financiación a través de Internet, que incluyó solicitar un rescate por información robada ante Gobiernos como

empresas, o más conocidos como ataques *ramsonware*, *carding*, *phishing*, *pharming*, entre otros (Cárdenas, 2022, p. 16).

Uso del Internet

El Internet se ha convertido en un medio muy poderoso para los ciberterroristas, debido a que muchas de sus bondades les han servido y les sirven para llevar a cabo su accionar ilícito, por ejemplo, su facilidad de acceso, bajo costo, falta de una buena regulación, la posibilidad de llegar a un número ilimitado de personas y la rapidez para divulgar la información. En tal sentido, el Internet es una ventaja estratégica para este grupo de delincuentes, lo cual le permite difundir sus ideas radicales, crear miedo y sensación de inseguridad en el mundo.

Las páginas web terroristas suelen ser utilizadas para subir videos, imágenes y difundir vía *online* instrucciones de cómo fabricar bombas y cómo realizar ciberataques. Existe la aplicación "E-jihad" con la cual un usuario puede realizar ciberataques de baja intensidad (DDoS) contra objetivos en Internet (Cárdenas, 2022, p. 25). Es preciso mencionar que, los ciberterroristas también utilizan la Web para, en caso de necesitar información o capacidades tecnológicas, contactar *hackers*, sindicatos del crimen organizado y cibercriminales, para lo cual utilizan los *chats* clandestinos que pululan en el ciberespacio.

En el 2003, el grupo terrorista Al Qaeda realizó una campaña de reclutamiento *online* a fin de reunir a personas que estuvieran dispuestas a viajar a Iraq y atacar a las fuerzas estadounidenses que se establecieron allí.[2]

Entre el 2008 y el 2009, fue condenado a prisión el físico nuclear Adlène Hicheur por

Imagen propia creada con fotografías de internet

2 Esta información fue reportada por el Instituto SITE (Search for International Terrorist Entities), grupo de inteligencia estadounidense.

haberse confabulado y haber ayudado a preparar un acto terrorista. Se dice que apoyó intelectual y logísticamente a Al Qaeda en el Magreb islámico, al Frente Mundial de Medios de Información Islámicos, y al Centro Rafidayin mediante mensajes secretos cifrados.[3]

Podemos señalar que, el conocimiento es uno de los instrumentos más importantes que utiliza el ciberterrorismo y la guerra de información. Asimismo, las herramientas que emplea, y aquellas a las que puede acceder un ciberterrorista, se encuentran al alcance; mientras que el conocimiento de los sistemas informáticos y sus debilidades para contrarrestar los actos terroristas no están disponibles o son de muy remoto acceso.

Entre las tecnologías utilizadas en la difusión de propagandas y mensajes, mencionadas por Llongueras, podemos señalar las siguientes:

a. Encriptación de mensajes y ficheros.
b. Esteganografía. Codifica mensajes en el interior de imágenes, ficheros u otros mensajes.
c. E-Grupos. Servicio ofrecido por una ISP para usuarios con los mismos intereses para intercambiar mensajes. El administrador del grupo decidirá si este es abierto o protegido con contraseña, por ejemplo "Jehaad" y "The Jihad Group" de Yahoo.
d. E-mail Dead Drops. Es la distribución de un nombre de usuario y contraseña para una cuenta de *mail* para miembros de células terroristas, en la que escriben mensajes y lo guardan en la cuenta. Este mensaje nunca es enviado *online*, queda guardado en el borrador de mensajes, con lo cual no se puede seguir la dirección IP o su geolocalización.
e. Hydra Web Links. Consiste en tener varios *links*, que son direccionados a un mismo video o mensaje, el cual se encuentra publicado en una página web o en un *e-mail chat room*. El usuario lo copia y cuelga en otro foro y *websites* para, así, evitar que el mensaje pueda ser interceptado por las autoridades.
f. Spam mimicking. Los terroristas visitan este sitio web y proceden a incrustar, integrar u ocultar mensajes confidenciales en el *spam*. (2016, p. 39)

3 Fuente extraída del diario *El País* del 15 de enero del 2016, en el que también se menciona que dictaba clases en Brasil. https://elpais.com/internacional/2016/01/13/actualidad/1452715986_096641.html

El Estado Islámico ha hecho un uso intensivo del Internet para afianzar su fuerza y poder, lo cual lo ha diferenciado del resto de grupos yihadistas. Este uso le ha permitido promover su causa, reclutar nuevos adeptos y financiamiento. Esta tendencia no va a desaparecer, por el contrario, es de temer que los demás grupos radicales sigan su ejemplo y utilicen las mismas bondades que ofrece el ciberespacio para sus actividades criminales.

Las ventajas del Internet han sido utilizadas en el ciberespacio para comprar vulnerabilidades *zero day*, infiltrarse en sistemas y extraer información para manipularla, difundir propaganda a través de *blogs*, foros, Facebook, Twitter y de las revistas digitales *Dabiq y Kybernetiq*, así como la difusión constante de la sensación de miedo en Occidente, creando una percepción de que el Daesh[4] es una amenaza continua y permanente al sistema de vida occidental.

> Daesh construyó su propio centro de medios de alta tecnología denominado Al-Hayat, conocido por producir videos de tortura, como el video que muestra la decapitación de James Foley. También, produce *Dabiq*, una entrevista de propaganda. Todo el contenido en línea se sube a los servidores de texto anónimo y es difundido en las redes sociales por los partidarios de Daesh. (Llongueras, 2016, p. 40)

Comparación entre el terrorismo tradicional y el ciberterrorismo, y cómo combatir al ciberterrorismo

Terrorismo convencional	Ciberterrorismo
Objetivos que existen en el mundo físico: aerolíneas, edificios, individuos de alto perfil y personas de perfil bajo.	Objetivos que existen en el ciberespacio: telecomunicaciones, redes informáticas, redes de control.
Crea una amenaza física.	Crea una amenaza física y virtual.
Armas: explosivos, armas de fuego.	Armas: *software* malintencionado, armas EMP (manipulación o destrucción de datos).
Técnicas: bombas, secuestros y asesinatos.	Técnicas: destrucción "virtual" de blancos en el ciberespacio, desactivación del *software* del sistema, intrusión y destrucción de los sistemas de control.
Tamaño del grupo: grande = gran impacto, pequeño = impacto potencial menor.	Tamaño del grupo: grande = gran impacto, pequeño = gran impacto potencial.
Gran inversión para obtener un gran impacto.	Poca inversión para obtener un gran impacto.
El riesgo físico es alto para los terroristas.	El riesgo físico es mínimo para los terroristas.

4 También conocido como Estado Islámico.

Valor del patrocinio estatal: dinero, equipo, entrenamiento, apoyo a la inteligencia y transporte.	Valor del patrocinio estatal: inteligencia.
Papel de los medios: crítico.	Papel de los medios: moderado.
Legislación establecida.	Falta de legislación.
Los requisitos de Intel / Info para el éxito son bajos.	Los requisitos de Intel / Info para el éxito son vitales.
Comunicaciones vitales para el éxito, y presenta una vulnerabilidad.	Comunicaciones vitales para el éxito y normalmente seguras (encriptación conectividad global).
El potencial de interrupción es moderado. Los ataques coordinados / distribuidos son complicados.	Potencial de interrupción es inmenso. Coordinación / ataques distribuidos relativamente fáciles.
Tipo de grupos: nacionalistas separatistas, ideológicos, exiliados, patrocinados.	Tipo de grupos: nacionalistas separatistas, ideológicos, exiliados, patrocinados por el Estado.
La presencia física es requerida para que el ataque tenga éxito. Las fronteras importan.	La presencia física no es necesaria para que el ataque tenga éxito. Fronteras inexistentes.
Attack has effects.	*Attack can have either focused of diffuse effects.* (Llongueras, 2016, pp. 20 y 21)

Ventajas y desventajas que alcanzó el ciber Yihad

Este grupo terrorista ha logrado obtener muchas ventajas en el ciberespacio, sobre todo en Internet, entre las que destacan:

a. Causar un efectivo daño económico.
b. Afianzar una guerra asimétrica.
c. Provocar un "cibermiedo" o una notoria ansiedad en el ciberespacio.
d. Aprovechar las vulnerabilidades de los sistemas.
e. Acceder a ciberarmas mediante *open source*.
f. Realizar operaciones a distancia sin problemas.
g. Dificultad para ser localizado (trazabilidad); anonimato, dificultad para ser encontrado.
h. Disminución de bajas físicas en operaciones contra objetivos occidentales.

Asimismo, ha presentado algunas desventajas:

a. Necesidad de gran preparación y conocimiento técnico para realizar determinados ciberataques.
b. Los ciberataques complejos no llegan a ser públicos por su alto riesgo para la seguridad nacional del país atacado y el sesgo moral que provocaría en la población, por ejemplo, los ciberataques a centrales nucleares.
c. Acceder a ciberarmas.

El Daesh no ha sido el primer grupo yihadista en utilizar Internet para sus fines ilícitos, pero sí se le considera el primero que ha logrado su transformación. Para Llongueras, en sus inicios, el Estado Islámico era un grupo yihadista más; sin embargo, gracias al Internet y las TIC, ha logrado diferenciarse del resto y ha conseguido hacerse conocido y temido a nivel mundial, convirtiéndose en una marca global.

Asimismo, ha obtenido, mediante el Internet, la captación de jóvenes alrededor del mundo, con los cuales, ha creado un vínculo y sensación de pertenencia al Daesh *online*. Igualmente, ha conseguido que cualquier persona pueda ayudar a la organización, moral y económicamente. El Estado Islámico ha logrado descentralizar, mediante la propaganda por Internet, sus objetivos, utilizando el *crowdsourcing* para difundir su ideología. Así también, las redes sociales han sido utilizadas como medios para llevar a cabo operaciones psicológicas en favor del Estado Islámico. Se podría decir que, el Internet es el centro de mando y control preferido por este grupo terrorista.

Combatir al ciberterrorismo es tarea de todos

Como bien lo señala Marín, en la actualidad, todas las personas deben saber cómo enfrentar el ciberterrorismo, sobre todo los padres a efectos de evitar que sus hijos sean reclutados por estas organizaciones criminales. En tal sentido, es crucial conocer el *modus operandi* de los terroristas, a fin de analizar los riesgos, saber autoprotegerse y cómo reaccionar para lograr aumentar las probabilidades de supervivencia y/o protección durante un atentado terrorista yihadista.

Muchos medios de comunicación, así como plataformas digitales han tratado de censurar la propaganda terrorista, pero lo cierto es que no todos lo han logrado. Asimismo, en el Internet denominado "visible"[5] de acceso general, existe una mayor protección respecto al contenido que se publica; sin embargo, existen puertas traseras o Internet invisible que no es capaz de tener un control real de la propaganda que se pueda trasmitir por dicho medio.

Así también, Google ha desarrollado *The redirect method*, el cual consiste en redireccionar el *spam mimicking*, utilizando herramientas de orientación de AdWords y los videos de YouTube cargados por personas de todo el mundo

5 Se le denomina visible debido a que también existe un internet denominado "dark web" o "deep web", al que solo tienen acceso ciertos grupos, por lo general aquellos que se encuentran al margen de la ley.

para hacer frente a la radicalización en línea. Incluso, frente a la oposición que realiza Twitter y Facebook, el dominio de las redes sociales por parte de Daesh continúa creciendo.

Sin embargo, lo cierto es que los Estados se niegan a cooperar de manera intensiva y eficiente para contrarrestar el ciberterrorismo y, en general, cualquier amenaza que se presente en el ciberespacio, debido a que cada uno quiere mantener su autonomía y soberanía en su territorio digital. Esa es la razón por la cual, a la fecha, no existe un tratado internacional sobre seguridad cibernética y ciberdefensa.

Por lo tanto, aún queda mucho por hacer. Esperemos que, así como las TIC y el Internet han sido utilizados de manera indebida, también sean estas las herramientas que nos proporcionen las salidas más adecuadas para contrarrestar el problema del ciberterrorismo lo más rápido; pero por ahora, solo nos queda aguardar.

Conclusiones

1. El terrorismo, como ideología, aún sigue presente en el mundo, y es uno de los problemas más críticos que deben afrontar las naciones del mundo.
2. El terrorismo utiliza ahora el ciberespacio para expandir sus horizontes.
3. Si bien el ciberterrorismo, en principio, produce disrupciones de páginas web, esto no significa que su utilización pueda causar daños radicales y destructivos contra infraestructuras del Estado y con consecuencias fatales.
4. El Internet y las TIC se han convertido en herramientas necesarias para la humanidad, pero también son armas utilizadas por los ciberdelincuentes y ciberterroristas para causar pánico y terror a nivel mundial.
5. Las principales formas de utilizar el Internet por los ciberterroristas son los siguientes: propaganda, publicidad, reclutamiento y financiación.
6. No existe por el momento una normativa internacional para ser utilizada en el ciberespacio contra actos perpetrados por los ciberdelincuentes y ciberterroristas.
7. No es posible contrarrestar a cabalidad este tipo de amenaza a la seguridad internacional, así que, solo queda aprender a vivir con ella. La unión de los Estados y naciones será un paso decisivo para afrontar este flagelo si queremos alcanzar la paz mundial.

8. Por ahora, debemos continuar conviviendo con este peligro latente llamado terrorismo y su forma de actuar a través de los ciberterroristas, mientras se encuentra una forma de lograr su neutralización y radicalización permanente.

Referencias

1. CÁRDENAS, María José. "Actividades Terroristas en el Ciberespacio". *Lisa News*. 2022. Actualizado el 27 de mayo de 2022. Disponible en: https://www.lisanews.org/ciberseguridad/actividadesterroristas-en-el-ciberespacio/.
2. GONZÁLES, E. "El laboratorio del miedo. Una historia general del terrorismo. Las oleadas históricas de la violencia terrorista: una reconsideración". *Revista de Psicología Social*, n.º 24 (2). 2012. P. 119-137.
3. LIBERTAD DIGITAL. 2005. https://www.libertaddigital.com/nacional/definicion-deterrorismo-segun-los-expertos-de-la-onu-1276246052/
4. LLONGUERAS, Adrianna. "Ciber Yihad y el Estado Islámico". 2016. file:///E:/02%20master%20en%20seguridad%20Y%20defensa02%20segundo%20Semestre/escenarios%20internacionales%20para%20la%20defensa/actividad/Bibliografia/Ciber_YIihad_el_estado_islamico_terrorism.pdf
5. MARIN, Gerard. "Curso de Introducción al Terrorismo Yihadista con Protocolos de Autoprotección". *Lisa News*. Disponible en: https://www.lisanews.org/formacion/curso-de-terrorismo-yihadistaprotocolos-consejos-de-autoproteccion/
6. PONS, Vicente. "Internet, la nueva era del delito: ciberdelito, ciberterrorismo, legislación y ciberseguridad". *Revista Latinoamericana de Estudios de Seguridad*. 2017. Disponible en: https://doi.org/10.17141/urvio.20.2017.2563
7. RAPOPORT, D. C. "Las cuatro oleadas del terror insurgente y el 11 de septiembre". En REINARES, F. y ELORZA, A. (coord.) *El Nuevo terrorismo islamista: del 11-S al 11-M*. 2004. P. 45-74.
8. PÉREZ, Emmanuel. Observatorio Internacional de Estudios sobre terrorismo: *Orígenes y evolución del territorio Yihadista*. 2015.