ieee.es
Instituto Español de Estudios Estratégicos
1970 — 2020

Documento
Opinión

106/2020 3 de septiembre de 2020

*Amanda Pérez Gómez**

Ciberterrorismo, ¿una nueva amenaza?

Visitar la WEB Recibir BOLETÍN ELECTRÓNICO

Ciberterrorismo, ¿una nueva amenaza?

Resumen:

El ciberespacio es un medio incontrolable con un alcance que supera barreras, lenguas e identidades, sirviendo de refugio a criminales y terroristas, quienes han encontrado en este una vía de fácil acceso y operatividad. No quedándose atrás las organizaciones terroristas que tan frecuente e incesantemente amenazan a las sociedades occidentales, poniendo en evidencia la necesidad de implantar, por parte de nuestros gobiernos, medidas preventivas en todos los ámbitos posibles. La única forma de afrontar esta modalidad terrorista es bajo la prospectiva, evitando así la puesta en peligro de infraestructuras críticas cuyo ataque supondría una rotura de alcance inimaginable en nuestra sociedad.

Palabras clave:

Ciberterrorismo, hacktivismo, cibercalifato, terrorismo, yihadismo, infraestructuras críticas.

Cyberterrorism, a new threat?

Abstract:

Cyberspace is an uncontrollable means, with a scope that overcomes barriers, languages, and identities, serving as a refuge for criminals and terrorists, who have found in it a way of easy access and operability. Not lagging the terrorist organizations that so frequently and incessantly threaten Western societies, highlighting the need for our governments to implement preventive measures in all possible areas. The only way to confront this terrorist modality is by looking into the future, thus avoiding the endangered of critical infrastructures whose attack would entail a break of unimaginable scope in our society.

Keywords:

Cyberterrorism, hacktivism, cyber caliphate, terrorism, Jihadism, critical infrastructures.

Cómo citar este documento:

PÉREZ GÓMEZ, Amanda. *Ciberterrorismo, ¿una nueva amenaza?* Documento de Opinión IEEE 106/2020.
http://www.ieee.es/Galerias/fichero/docs_opinion/2020/DIEEEO106_2020AMAPER_ciberterrorismo.pdf y/o enlace bie[3] (consultado día/mes/año)

Introducción

Las nuevas tecnologías se han extendido a lo largo de la última década de manera asombrosa, llegando a ámbitos inhóspitos y, en muchas ocasiones, facilitándonos la vida. Sin embargo, una vez más, este tipo de avances también ha sido aprovechado por actores cuyos fines pretenden dañar o alterar el orden social, como es el caso de las organizaciones terroristas. Siendo estos conscientes de que nuestra sociedad aún no está lo suficientemente preparada como para afrontar o frenar un atentado a través de estos medios, al confeccionarse y ejecutarse en un espacio tan sumamente amplio como es el ciberespacio, siendo muy fácil de camuflar, mantener en el anonimato y lo que es más peligroso, superar largas distancias y fronteras en un solo clic.

Sin embargo, existe la certeza de que organizaciones terroristas como el Estado Islámico o Al Qaeda, hasta ahora, no han supuesto una amenaza en este ámbito, y que todos sus intentos para introducirse en él han sido nulos o de escaso alcance. Parece ser que el espectáculo y los atentados visuales siguen siendo su principal vía y, por ende, nuestra mayor preocupación.

Este ensayo lo que pretende es exponer un peligro inherente en nuestra sociedad actual y, sobre todo, mostrar la urgente necesidad de actuar de manera prospectiva, adelantándonos a los acontecimientos, yendo un paso por delante y así poder evitar futuros ataques que puedan minar ciudades enteras. Un claro ejemplo de ello es la COVID-19, algo tan básico que ha paralizado la economía mundial y que está matando millones de personas de manera imparable.

Ciberamenazas

Tomando por ciberamenazas «todas aquellas disrupciones o manipulaciones maliciosas que afectan a elementos tecnológicos. Caracterizadas por su diversidad tanto en lo que concierne a capacidades como a motivaciones. Afectando a todos los

ámbitos de la Seguridad Nacional: Defensa Nacional, seguridad económica o la protección de infraestructuras críticas, sin distinción de fronteras»[1].

Debido a su carácter transversal es necesaria una cooperación entre las Administraciones públicas, el sector público y privado y la propia sociedad, al ponerse en grave peligro los derechos humanos, la defensa, la economía y el desarrollo tecnológico. Para poder conseguir una buena estrategia de seguridad es necesario un plan integral que vaya evolucionando y se vaya adaptando a este tipo de amenaza que lleva la iniciativa y que se multiplica por el efecto llamada de su alto nivel de impunidad.

En los ámbitos de defensa, tanto la *Deep Web* como la *Dark Web*, constituyen una importante fuente de ciberdelincuencia, en este caso en particular, se enfatizará sobre el ciberterrorismo y hacktivismo.

Amenazas híbridas y cibercriminalidad

Las tecnologías digitales suponen una vía de fácil acceso para actividades y negocios maliciosos e ilegales, debiendo ser obligatoriamente controlados o prevenidos, ya que la ejecución de estos puede conllevar un daño a los derechos y libertades, suponiendo serias amenazas y desafíos a la Seguridad Nacional[2].

Estos medios se están convirtiendo en una vía para la expansión de amenazas híbridas, entendiendo por estas aquellas «acciones coordinadas y sincronizadas, dirigidas a atacar de manera deliberada las vulnerabilidades sistemáticas de los Estados democráticos y las instituciones, a través de una amplia gama de medios, ya sean acciones militares tradicionales, ciberataques, operaciones de manipulación de la información o elementos de presión económica»[3]

[1] Ministerio de la Presidencia, Relaciones con las Cortes e Igualdad. *Estrategia Nacional de Ciberseguridad*, Gobierno de España, 2019, pp. 23-24.

[2] Ibidem, pág. 24.

[3] Ibidem, pág. 25.

Por otro lado, la cibercriminalidad, un problema de primer orden en lo relativo a la seguridad ciudadana, un tipo de amenaza cada vez más extendida y generalizada, que afecta a instituciones, empresas y ciudadanos, indistintamente[4].

En lo relativo a los grupos terroristas, encuentran en el ciberespacio un lugar propicio para su financiación, cuyo fin es realizar ciberataques (por grupos hacktivistas), propaganda, radicalización de individuos, divulgación de técnicas y de herramientas para la comisión de atentados, superando barreras y distancia geográfica. Esto supone un alto riesgo hacia las infraestructuras críticas, las cuales, en caso de sufrir un ataque, supondría un colapso de innumerables dimensiones en la sociedad o inclusive a nivel transnacional[5].

Diferencia entre ciberterrorismo y hacktivismo

Como se ha mencionado anteriormente, la diana de este tipo de ataques son las infraestructuras críticas. Un simple y aislado ataque hacia una de ellas derivaría en un daño mucho mayor que una serie de ataques múltiples en otro tipo de objetivos. A lo largo de los años, numerosos ciberataques han sido atribuidos a hackers simpatizantes de causas terroristas. Pero ¿cómo podemos diferenciar el hacktivismo y el ciberterrorismo? ¿En qué consiste cada uno?

Hacktivismo

El término hacktivismo, surge de la combinación de *hacking*[6] y activismo, entendiéndose como una articulación entre el activismo y el uso de las herramientas hacker para protestar en Internet; es decir, el uso ilegal o legal de herramientas digitales para fines políticos y de protesta[7].

[4] Ministerio de la Presidencia, Relaciones con las Cortes e Igualdad. *Estrategia Nacional de Ciberseguridad*, Gobierno de España, 2019, p. 25.

[5] Ibidem, p. 26.

[6] Irrupción ilegal a sistemas computacionales con fines criminales.

[7] MOHAR, E. “Qué es el hacktivismo?”, *Muy Interesante*, 31 de mayo de 2018. Disponible en: https://www.muyinteresante.com.mx/ciencia-y-tecnologia/hacktivismo/

Es considerada como un ejemplo leve de *Netwar* (infoguerra), por lo que no se interpreta como una acción criminal, sino más bien como «una forma legítima de protesta que se concentra en objetivos gubernamentales o empresariales, para incitar un boicot, la desobediencia civil digital o convocar un mitin ciberespacial. La red es usada como un agente para la justicia social a través de acciones de protesta»[8].

Existen diferentes formas de hacktivismo: en primer lugar, la destrucción de páginas web, es decir, boicotearlas, abarcando desde caídas de sistemas hasta la difusión de información falsa; *Web Sit-ins*, bombardeos de email, «espejeo de sitios», «geobombardeo» y, finalmente, *doxing*[9].

Las principales características por las cuales el hacktivismo es llamativo y altamente provechoso para el terrorismo son su fácil accesibilidad, el reducido riesgo personal debido al anonimato, el alto impacto tanto social como mediático de sus acciones y el amplio abanico de capacidades que ofrece superando distancias geográficas, culturales o incluso lingüísticas[10].

Ataques DOS (Deny Of Service)

La denegación de servicio (DOS, por sus siglas en inglés) es «la apropiación exclusiva de un recurso o servicio con la intención de evitar cualquier acceso de terceros. También se incluyen en esta definición los ataques destinados a colapsar un recurso o sistema con la intención de destruir el servicio o recurso»[11]. Una definición más restrictiva es la relativa a los ataques de denegación de servicio en redes IP, «consecución total o parcial (temporal o totalmente) del cese en la prestación de servicio de un ordenador conectado a Internet. Un ataque exitoso contra el protocolo IP

[8] PINO, E. K. "El Hacktivismo: entre la participación política y las tácticas de subversión digital*", Razón y palabra* (88), 26, 2014-2015, p. 4.

[9] MOHAR, E. "Pero ¿qué es un hacktivista?", *Muy Interesante*, 31 de mayo de 2018. Disponible en: https://www.muyinteresante.com.mx/ciencia-y-tecnologia/hacktivismo/

[10] TORRES-SORIANO, Manuel R. *El hacktivismo como estrategia de comunicación: de Anonymous al cibercalifato.* Instituto Español de Estudios Estratégicos (IEEE) Cuadernos de Estrategia, ISSN 1697-6924, Nº. 197, 2018 (Ejemplar dedicado a: *La posverdad. Seguridad y Defensa*), pp. 202-203.

[11] ALVAREZ, G. V. *Seguridad en redes IP: DOS/DDoS,* Universidad Autónoma de Barcelona, Departamento de informática. Universidad Autónoma de Barcelona. 2003, p. 37.

se convierte inmediatamente en una amenaza real para todos los ordenadores conectados a Internet»[12].

Ataques DDoS (Denegación de Servicio Distribuido)

Este tipo de ataques consiste en la denegación de un servicio en el que existen múltiples focos distribuidos y sincronización que focalizan su ataque en un mismo destino. Normalmente, el modelo más utilizado es TRINOO, que implementa la denegación de servicios mediante un modelo jerárquico maestro. Lo más normal es que los ordenadores intervenidos pertenezcan a grandes corporaciones o entidades, que poseen una amplia red, pasando fácilmente desapercibidos entre los miles de ordenadores que pertenecen a la misma. Una vez infectado el núcleo principal, se procede al *scanning* y contagio del resto de ordenadores que conforman la red[13].

Ciberterrorismo

Al igual que ocurre con el término hacktivismo, ciberterrorismo proviene de la combinación de lo relativo al ciberespacio y el terrorismo.

El término ciberterrorismo se estableció, en 1980, por Barry Collin, bajo la percepción de una convergencia entre los dos mundos, el virtual y el físico. Posteriormente, académicos tales como Mark M. Pollitt, han añadido una definición más concreta sobre el fenómeno: «Ataque predeterminado, políticamente motivado, contra información, sistemas y programas informáticos y datos a través de la red, como acto violento contra objetivos no combatientes por organizaciones o agentes clandestinos»[14].

El ciberespacio es frecuente testigo de ciberataques por parte de actores no estatales, siendo este factor el elemento diferenciador con la ciberguerra, la cual está dirigida por los propios Estados. Sin embargo, estos actores no estatales no pueden llegar a obtener la consideración de ciberterrorismo por dos motivos: en primer lugar, los ataques más dañinos y destructivos no están motivados por razones políticas ni sociales, en la mayoría de ellos se trata de un móvil lucrativo; en segundo lugar, los

[12] Ibidem

[13] Ibidem, pp. 48-49.

[14] POLLITT, M. M. *Cyberterrorism: Fact or Fancy,* Computer Fraud & Security 2. 1998, p. 9.

ataques han sido conectados con objetivos políticos y sociales sin llegar a ser intimidatorios ni nocivos, siendo ejecutados por activistas, no por terroristas. Debido a esto, lo más común es clasificarles como hacktivismo, no ciberterrorismo, para que puedan ser considerados como tal, deben conseguir crear el mismo terror o efectos que generan los actos físicos del mismo fenómeno.

Los principales objetivos de este tipo de ataques son infraestructuras críticas. Estas acciones afectan a muchos factores más que la propia vida humana, como sucedería en un atentado convencional[15].

Según el Center on Terrorism and Irregular Warfare (CTIW) en el Naval Postgraduate School (NPS) en California, el ciberterrorismo es una amenaza futura, la cual debe ser prevenida y a la cual nos debemos anticipar. A través de estudios se ha demostrado y evidenciado la existencia de una alianza entre terroristas y hackers, con la cual ambos buscan causar daño en recursos y fuentes de información. Sin embargo, la detección o esclarecimiento de esta relación, puede ser complicada[16].

El cibercalifato: «hacktivismo parásito de simbología proislamista»

Además de los más conocidos usos que el yihadismo hace de Internet, como la distribución de propaganda, la publicación de vídeos o adoctrinamiento y captación de fieles, el hacktivismo se ha abierto una puerta en este mundo convirtiéndose en una posible peligrosa arma a utilizar por este movimiento.

Los ciberyihadistas conducen sus objetivos hacia recopilaciones de inteligencia y de información. Un ejemplo de ello es el proporcionado por Magnus Ranstorp, el cual afirma que Al Qaeda obtuvo información acerca de los movimientos, operaciones y geolocalización de diferentes actores al servicio del Gobierno norteamericano en el mundo árabe, gracias al acceso a una cuenta de email de un diplomático estadounidense[17].

[15] DENNING, D. E. A *View of Cyberterrorism Five Years Later*, Calhoun: Dudley Knox Library at NPS, 19, 2006, pp. 2-3.

[16] PINO, E. K. "El Hacktivismo: entre la participación política y las tácticas de subversión digital*", Razón y palabra* (88), 26, 2014-2015, pp. 5-6.

[17] Ibidem, p. 9.

Cyber Caliphate Army (CCA) fue uno de los primeros grupos ciberterroristas apoyando al Estado Islámico, fundado por el hacker británico Abu Hussain al Britani (Junaid Hussain) quien, a los 15 años, ya había creado un grupo que posteriormente se unió a la lucha por la liberación de Palestina, hackeando entidades israelíes, británicas y estadounidenses. Tras una temporada en prisión, se unió a las filas del Dáesh en Siria, pasando a ser uno de los líderes de propaganda, reclutando hackers y creando el Cyber Caliphate Army, además de Islamic State Hacking Division (ISHD)[18]. Cabe mencionar que, tal y como indica Enrique Fojón Chamorro en un artículo para el Real Instituto el Cano, debido al escaso conocimiento acerca del cibercalifato, no es posible asegurar a ciencia cierta que los cibergrupos mencionados pertenezcan al Estado Islámico, siendo más probable su calificación como meras organizaciones pro-Dáesh[19]. Tras la muerte de Junaid y estableciéndose Siful Haque Sujana como nuevo líder, la actividad de este grupo hacktivista se vio fuertemente menguada, quedando reducida a actos individuales. En 2016, se crea Sons Caliphate Army (SCA), como subgrupo del CCA, reclamando al Dáesh la comisión de más de 15 000 ciberataques en cuentas de Twitter y Facebook[20].

El hacktivismo yihadista tiene un carácter disperso, compartiendo mismos objetivos y metodología, sin embargo, los activistas partícipes son propensos a agruparse en multitud de grupúsculos, efímeros, no coordinados entre sí, resultando irrelevantes[21].

El informe publicado por el CCN-CERT en el 2018 indica que «las manifestaciones en el ciberespacio de acciones de ciberterrorismo de raíz fundamentalista fueron principalmente debidas a simpatizantes de ISIS». En cambio, no hay evidencias o hechos que constaten que puedan suponer una amenaza en el desarrollo de ciberataques. Como se ha venido observando en los últimos años, sus atentados se caracterizan por la aleatoriedad, cuando la planificación y el desarrollo previo para llevar a cabo ciberataques es primordial y estrictamente necesario.

[18] TORRES-SORIANO, Manuel R. *El hacktivismo como estrategia de comunicación: de Anonymous al cibercalifato.* Instituto Español de Estudios Estratégicos (IEEE) Cuadernos de Estrategia, ISSN 1697-6924, Nº. 197, 2018 (Ejemplar dedicado a: *La posverdad. Seguridad y Defensa*), p. 218.

[19] CHAMORRO, E. F. "El Estado Islámico y la ciberguerra", *Real Instituto el Cano*, 3, 2015, p. 1.

[20] GIANTAS, D. (s.f.). "From Terrorism to Cyber-terrorism: The Case of ISIS", *Piraeus: Helenic Institute of Strategic Studies,* University of Peloponnese, Greece, p. 10-12.

[21] TORRES-SORIANO, *El hacktivismo como estrategia de comunicación: Op.cit.*, p. 222.

El Estado Islámico ha demostrado estar interesado en el desarrollo de esta vía de ataque, a pesar de no haber llegado más allá de meros ataques DDoS o desfiguraciones, todos ellos de naturaleza propagandística, la cual podía ser encontrada en la *Surface Web*. A pesar de ello, conociendo su potencial en el ámbito del reclutamiento y su poder ofensivo, debe establecerse una mirada prospectiva sobre el cibercalifato y su creciente peligrosidad[22]. «Estado Islámico parece estar priorizando la captación de jóvenes europeos con conocimientos y formación en nuevas tecnologías con el objetivo de crear su propio "ciberejército"»[23].

El ciberterrorismo es tan débil que el término «cibercalifato», según el informe del CCN-CERT de 2020 sobre Hacktivismo y ciberyihadismo, se considera carente de vinculación real con ninguna organización terrorista yihadista. El denominado cibercalifato es un término utilizado especialmente por actores individuales, de procedencia india o indonesia, que realizan ciberataques por desfiguración contra sitios web, insertando menciones al Dáesh como medio de provocación. Concretan en dicho informe que la terminología correcta a emplear sería «hacktivismo parásito de simbología proislamista»[24].

Un ejemplo de este tipo de hacktivismo que incluye contenido islamista en sus ataques, es el caso de Mujahidin313, identidad que realizó desfiguraciones en sitios web de diferentes partes del mundo, durante 2018, en los que incluía contenido proislamista a favor de la creación de un califato islámico, con la característica de ser contrario al Dáesh. Desde junio de 2019, no ha vuelto a dar señales de actividad[25].

Al igual que Mujahidin313, otras entidades han utilizado grafismo o contenido proislamista a modo de provocación, durante el año 2019, entre ellos Munashir Cyber Section, con desfiguraciones web en Sudáfrica; Morrocanwolf, incorporando menciones al Dáesh, o marwan007, quien incluyó en el ciberataque imágenes de yihadistas armados[26].

[22] CCN-CERT IA-09/18. "Ciberamenazas y Tendencias Edición 2018", Centro Criptológico Nacional, 2018, pp. 21-22.

[23] CHAMORRO, E. F"El Estado Islámico y la ciberguerra", *Real Instituto Elcano*, 3, 2015, p. 2.

[24] Centro Criptológico Nacional CCN-CERT. "Informe anual 2019: Hacktivismo y ciberyihadismo", Centro Criptológico Nacional, 2020, p. 49.

[25] Ibidem, p. 49.

[26] Ibidem, pp. 50-51.

En cuanto a aquellos que han hecho uso del término «cibercalifato» en sus ciberataques, ayudando así a la propagación del concepto, encontramos la desfiguración en manos de 0x.Terrorist y 0x.Shadow, en enero de 2019, incluyendo alusiones al Dáesh y al United Cyber Caliphate. De igual forma ataques webs bajo el pseudónimo de Caliphate Cyber Shield en India y Canadá durante el mismo año, y el ataque por denegación de servicio a la policía del estado de Karnataka en India, por la identidad Cyber Revenge Army[27].

Más allá de un cibercalifato, el uso de Internet con fines yihadistas puede resumirse en los siguientes puntos:

1. Propaganda: ya sea a través de comunicados o mensajes, en revistas, medios audiovisuales o tratados, impartiendo instrucción ideológica o práctica, explicando, justificando o promoviendo las actividades terroristas[28].
2. Financiación.
3. Adiestramiento: ejemplo de ello tenemos la revista *Inspire,* propiedad de Al Qaeda, con el objetivo declarado de permitir a los musulmanes entrenarse para la yihad en su casa[29].
4. Planificación: medidas preparatorias que abarcan desde la obtención de instrucciones sobre métodos de ataque, hasta la recopilación de información en relación con el blanco escogido para el atentado[30].
5. Ejecución: siendo el ciberespacio un medio comunicativo jamás ante visto, aportando ventajas logísticas y reduciendo las probabilidades de detección. Además de ser imprescindible para la adquisición de elementos necesarios en la ejecución de atentados[31].

[27] Ibidem, p. 51.

[28] "El uso de internet con fines terroristas", Oficina de las Naciones Unidas contra la Droga y el Delito, 174. 2013, p. 3.

[29] Ibidem, p. 8.

[30] Ibidem, p. 10.

[31] Ibidem, p. 12.

Infraestructuras críticas

La Directiva 2008/114/CE del Consejo de 8 de diciembre de 2008 sobre la identificación y designación de infraestructuras críticas europeas y la evaluación de la necesidad de mejorar su protección, establece y determina, en su artículo 2.a), lo que se entiende por infraestructura crítica: «El elemento, sistema o parte de este, situado en los Estados miembros, que es esencial para el mantenimiento de funciones sociales vitales, la salud, la integridad física, la seguridad, y el bienestar social y económico de la población y cuya perturbación o destrucción afectaría gravemente a un Estado miembro al no poder mantener esas funciones», incluyendo en su apartado b) las «ICE» (infraestructuras europeas), las cuales, en caso de ser atacadas provocarían daños a, al menos, dos Estados miembros[32].

El mundo es un espacio interconectado, en el que la tecnología ha resultado ser al mismo tiempo, un factor de crecimiento y de riesgo. Centrándonos en lo relativo a las infraestructuras críticas y las posibilidades de ser atacadas a través de métodos cibernéticos, podemos encontrarnos con variaciones en su arquitectura, hallándonos frente a sistemas híbridos, sistemas aislados de Internet (estando interconectadas entre ellas a través de una red interna, quedando así protegidas de un ataque de este calibre) y, en tercer lugar, los sistemas de control SCADA, al cual se puede acceder desde Internet. En este último caso cabe decir que este tipo de infraestructuras no están directamente gestionadas por este modelo de sistemas. Sin embargo, estos sí que sirven como puerta de entrada a las mismas, pudiéndose obtener información confidencial que facilite la elaboración de un ataque más sofisticado[33].

Para prevenirlos, son especialmente necesarios los análisis de riesgos (artículo 2.c de la Directiva), consistiendo en el estudio de las diferentes hipótesis sobre potenciales amenazas, examinando las vulnerabilidades y las posibles repercusiones del ataque a la infraestructura, es decir, entra en juego la mirada prospectiva, sobre la que se hace

[32] Directiva 2008/114/CE del Consejo de 8 de diciembre de 2008 sobre la identificación y designación de infraestructuras críticas europeas y la evaluación de la necesidad de mejorar su protección, DOUE-L-2008-82589 (Unión Europea 8 de diciembre de 2008).

[33] "Panda Security: Infraestructuras Críticas", obtenido de Panda Security: Infraestructuras Críticas, 30 de noviembre de 2016. Disponible en: https://www.pandasecurity.com/spain/mediacenter/src/uploads/2018/10/1611-WP-InfraestructurasCriticas-ES.pdf

inferencia en este artículo. Además de otro factor clave a tener en consideración llegados a este punto, la información sensible sobre protección de infraestructuras críticas (artículo 2.d de la Directiva), datos específicos que en caso de ser revelados pondrían en peligro la seguridad de estas[34].

Fue a partir de los atentados del 11 de septiembre en Nueva York cuando se vislumbró la especial importancia en lo relativo a la protección de ciertos objetivos, los cuales, en caso de ser atacados, ponían en grave peligro la seguridad ciudadana y estatal. Hasta ese momento, la protección de las infraestructuras críticas era competencia de la seguridad pública, sin embargo, hoy en día, en su mayoría se encuentran bajo la tutela del sector privado.

En el caso estadounidense, tras los ataques al *World Trade Center en 2001,* se creó el departamento de Seguridad Interior, modernizando y ampliando la seguridad en la materia. A nivel europeo, fue a partir de los atentados del 11 de marzo de 2004 en Madrid cuando se dio el paso definitivo, creándose el Programa europeo para la protección de infraestructuras críticas, en el cual se incluían propuestas para mejorar la prevención y respuesta ante atentados terroristas[35].

En comparación con otros riesgos, la evaluación de posibles atentados terroristas contra infraestructuras críticas supone un reto, sobre todo por la incertidumbre que gira en torno a ello. Como se alega en el informe *The protection of critical infrastructure against terrorist attacks: Compendium of good practices* publicado por las Naciones Unidas en 2018, la actividad terrorista evoluciona y se adapta a las medidas de seguridad que los Estados van aplicando, es decir, es un peligro dinámico y cambiante. Debido a ello, se asume la plena responsabilidad en las agencias de inteligencia, entrando en jaque el artículo 2.d de la Directiva 2008/114/CE, en torno a la protección plena de los datos confidenciales, que pueden poner en peligro a las propias infraestructuras[36].

---

[34] Directiva 2008/114/CE del Consejo de 8 de diciembre de 2008 sobre la identificación y designación de infraestructuras críticas europeas y la evaluación de la necesidad de mejorar su protección, DOUE-L-2008-82589 (Unión Europea 8 de diciembre de 2008).

[35] "Panda Security: Infraestructuras Críticas", obtenido de Panda Security: Infraestructuras Críticas, 30 de noviembre de 2016. Disponible en: https://www.pandasecurity.com/spain/mediacenter/src/uploads/2018/10/1611-WP-InfraestructurasCriticas-ES.pdf

[36] "The protection of critical infrastructures against terrorist attacks: Compendium of good practices", *UNITED NATIONS, OFFICE OF COUNTER-TERRORISM; INTERPOL*, 2018, pp. 33-34.

Los programas contraterroristas de protección de infraestructuras críticas deben tener en cuenta los diversos factores que engloban el problema, bien sean cambios geopolíticos, económicos o las relaciones entre las distintas organizaciones. En esta visión prospectiva del problema, es fundamental tener en cuenta los sistemas de alianzas, ya no solo en la cooperación a la hora del traspaso de información o prestación de otro tipo de ayuda, sino bajo la consideración de posibles atentados «reflejos» en países aliados, interconectados por la reciprocidad en sus puntos fuertes y al mismo tiempo en sus puntos débiles y de riesgo[37].

Conclusiones en relación con las medidas puestas en marcha

Una vez más la indefinición del término «terrorismo»[38] deja en evidencia la respuesta internacional ante el mismo. A pesar de que las Naciones Unidas haya establecido una Estrategia Global contra el Terrorismo (Resolución 60/288), es competencia de cada Estado el juicio y condena de los actos terroristas en base a su legislación. Por lo tanto, es muy difícil la cooperación internacional en este sentido. Debido a ello, los instrumentos legales universales, no definen los delitos de terrorismo en un derecho internacional, sino que simplemente establecen la obligación de cada Estado en perseguirlos y penarlos. Por lo que, focalizando este problema en torno al tema tratado, no existe un convenio universal que trate específicamente la prevención y control del uso de internet con fines terroristas.

En el ámbito europeo, existe el Convenio sobre la Ciberdelincuencia, cuya finalidad no es otra que la armonización legislativa en delitos de terrorismo y ciberdelincuencia. En este sentido, complementado por lo establecido en el Convenio Europeo para la Prevención del Terrorismo, es obligación de los Estados, miembros o no del Consejo de Europa, tipificar como delito la incitación pública, adoctrinamiento y adiestramiento a través de internet, además de una cooperación internacional de intercambio de información.

[37] "The protection of critical infrastructures against terrorist attacks: Compendium of good practices", *UNITED NATIONS, OFFICE OF COUNTER-TERRORISM; INTERPOL*, 2018, pp. 56-57.

[38] CORRAL, R. L. (s.f.). "El uso de las nuevas tecnologías por el terrorismo yihadista" (G. Civil, Ed.) *Cuadernos de la Guardia Civil* (Nº 54), 50-73, pp. 55-67.

La Unión Europea, ha intentado solventar el problema de la indefinición, a través de la Decisión Marco del 13 de junio de 2002, 2002/475/JAI, con la cual el Consejo de la Unión Europea proponía una armonización de dicha definición, en vistas al aumento de terrorismo yihadista. Medidas antiterroristas que se han visto ampliadas e intensificadas a partir de los atentados de París en 2014 y posteriores.

En el caso nacional, España, tras los atentados de los últimos años, modernizó el Código Penal en sus artículos dedicados a terrorismo, tipificando la difusión de ideas incitadoras, como es el adiestramiento, o la facilidad y la vía que suponen los medios cibernéticos, en la salida de *foreign fighters*. El Código Penal español ha definido como delitos de terrorismo, aquellas infracciones informáticas llevadas a cabo con la finalidad de adiestrar(se), obtención de documentos o archivos, cuando se acceda de manera frecuente a servicios que ofrezcan contenido idóneo para la incorporación a organizaciones o grupos terroristas, o el simple hecho de colaboración con los mismos.

Para hacer posible la cooperación internacional, existen una serie de instrumentos, como la Orden de Detención Europea, la Orden de Investigación, el Grupo Egmont de unidades de inteligencia financiera, INTERPOL o EUROPOL.

Como se ha mencionado, la peligrosidad actual del ciberterrorismo en relación con la comisión de posibles atentados contra infraestructuras críticas, es de un nivel muy bajo, al haber sido el límite máximo alcanzado por las organizaciones terroristas actuales del ciberespacio, ha sido la financiación, propaganda y adoctrinamiento, no llegando a utilizar esta vía para atentar. Bien es sabido que la mejor manera de detener y luchar contra el terrorismo es el uso de la inteligencia, implantar medidas prospectivas, que se adelanten a los actos, configurando una prevención real.

Como dijo Arturo Pérez Reverte «Siempre hubo Torres Gemelas, “troyas”» pero no se vieron como una diana para el terrorismo hasta aquel 11 de septiembre de 2001. Es necesario cambiar la forma de pensar, cambiar la mente a la de un terrorista y entonces será cuando las medidas antiterroristas serán eficaces y preventivas.

*Amanda Pérez Gómez**
Criminóloga
Alumna del Máster en Análisis y Prevención del Terrorismo
Universidad Rey Juan Carlos