Dossier Seguridad Internacional y Políticas de Defensa

Capacidades prospectivas y de defensa en la lucha contra el ciberterrorismo: análisis del caso español [1]

Prospective and Defense Capabilities against Cyberterrorism: the Spanish case

González-García, Abel; Girao González, Francisco José

Abel González-García
abel.gonzalez@udima.es
Universidad a Distancia de Madrid, España
Francisco José Girao González
fgirao@ucm.es
Universidad Complutense de Madrid, España

Relaciones Internacionales
Universidad Nacional de La Plata, Argentina
ISSN: 1515-3371
ISSN-e: 2314-2766
Periodicidad: Semestral
vol. 29, núm. 58, 2020
revista@iri.edu.ar

Recepción: 27 Enero 2020
Aprobación: 29 Junio 2020

URL: http://portal.amelica.org/ameli/journal/26/263615014/

DOI: https://doi.org/10.24215/23142766e097

Resumen: Los ciberataques y el cibercrimen (disrupciones con motivación económica o de intereses nacionales extranjeros) son una realidad diaria patente y en auge en el mundo. Dentro de los ciberataques se pueden encontrar casos referidos a ciberterrorismo, es decir, la unión del terrorismo y el ciberespacio (o la tecnología), con la finalidad de generar miedo o intimidar a una sociedad dirigiéndola hacia una meta ideológica. Se debate el concepto de ciberterrorismo. Tras el análisis de la amenaza, la pregunta que nos hacemos es si las capacidades preventivas (prospectivas y de defensa) de los Estados, tras el análisis concreto de España como miembro de la comunidad internacional, estarían preparadas para hacer frente a una amenaza de estas características en el futuro. Aquí hemos podido comprobar las diferentes capacidades existentes en España y conocer su grado de coordinación y colaboración para llegar a una serie de conclusiones sobre su idoneidad en la lucha de este fenómeno en plena expansión. El análisis se ha realizado a través de métodos prospectivos de escenarios posibles, donde cobran fuerza las funciones de difusión y captación, frente a ciberataques directos, aunque sin llegar a descartarlos en un futuro.

Palabras clave: ciberterrorismo, capacidades prospectivas, defensa, contraterrorismo.

Abstract: Cyberattacks and cybercrime (attacks with economic motivation or against national interests) are an actual daily reality in Spain and in entire the world. They may even be a part of cyberterrorism, which is the union of terrorism and cyberspace (or technology) to instill fear in people with an ideological goal. First, we will analyze the cyberterrorist threat and, second, we will ponder on whether the States have preventive capabilities (prospective and defense), by analyzing Spain's capabilities as a member of the International Community, and whether they would be prepared fight against this phenomenon. We have verified the different capabilities existing in Spain and we have presented their degree of coordination and collaboration. Finally, conclusions and future implications will be discussed. The prospective method is used and we discuss possible scenarios in cyberterrorism.

Keywords: cyberterrorism, prospective capabilities, defense, counterterrorism.

1. Introducción: el problema de la definición de ciberterrorismo.

La importancia de los ciberataques en el mundo es innegable y, en este sentido, Javier Candau Romero, Jefe del Departamento de Ciberseguridad del Centro Criptológico Nacional (CCN) español, adscrito al Centro Nacional de Inteligencia (CNI), detallaba a senadores y diputados españoles en septiembre de 2018 que los servicios públicos españoles sufren una media de 3000 ataques mensuales (Congreso de los Diputados, 2018). Además, los datos en el conjunto de los últimos años confirman un aumento en la incidencia de los ciberriesgos: en 2018 el CCN gestionó más de 38.000 ciberincidentes relacionados con la seguridad, con un aumento del 43,65% con respecto a 2017 (26.500 incidentes) (CCN-CERT, 2019: 108).

El aumento en la incidencia de los ciberataques es incuestionable, pero aquí lo que intentamos conocer es qué cantidad de estos ciberataques pueden formar parte del fenómeno del ciberterrorismo, y es donde surge el primer problema, ya que no podemos saber, por lo menos con los datos que se hacen públicos, cuáles de estas amenazas pueden llegar a formar parte de ataques ciberterroristas o intentos de estos, porque se desconoce la motivación de los atacantes en la mayoría de los casos.

Pero antes de entrar en el fondo del asunto, conviene que señalemos cuál es la definición de ciberterrorismo. De una manera simplista podemos resumirla en el encuentro del terrorismo con las tácticas propias del ciberespacio. Se puede comprobar que un problema complejo no puede quedar solo reducido a la unión de dos definiciones más, por un lado, terrorismo y, por otro, el ciberespacio. Para aclarar un poco más el asunto, la OTAN, por su parte, definió el ciberterrorismo en 2008 como "un ciberataque usando o explotando redes informáticas o de comunicación para causar una destrucción o disrupción suficiente para generar miedo o intimidar a una sociedad dirigiéndola hacia una meta ideológica" (Center of Excellence Defense Against Terrorism, 2008).

Ya en España, dentro de la Estrategia Nacional de Ciberseguridad (2019), se exponen los elementos concretos de los ataques ciberterroristas para complementar la definición, y se indica que

> los grupos terroristas tratan de aprovechar las vulnerabilidades del ciberespacio para realizar ciberataques o para actividades de radicalización de individuos y colectivos, financiación, divulgación de técnicas y herramientas para la comisión de atentados, y de reclutamiento, adiestramiento o propaganda. Íntimamente relacionado con ello, se halla la amenaza contra las infraestructuras críticas, con la posibilidad cierta de causar un colapso a través de las redes mediante una caída en cadena de los servicios esenciales.

Un aspecto que debemos destacar del fenómeno es que los atentados no son fines en sí mismos sino medios, como muestran De la Corte, Kruglanski, De Miguel, Sabucedo y Díaz (2007: 366-374):

> Los atentados terroristas (...) deberían ser interpretados (...) como la resultante de múltiples procesos de interacción social que tienen lugar a tanto a nivel intergrupal e intragrupal. Además, algunos de esos procesos de influencia se ejercen de forma deliberada y estratégica. Así, los publicistas profesionales se dedican a diseñar y aplicar campañas informativas con el objetivo explícito de influir sobre las actitudes y las pautas de compra de un amplio público. En cierto modo, los terroristas hacen algo parecido. Un viejo dicho anarquista definía el terrorismo como un tipo especial de propaganda: «la propaganda por el hecho». Se trata de una expresión bastante certera.

Por otra parte, Maras (2017: 386) considera que el uso de Internet por los terroristas se define erróneamente como ciberterrorismo. En realidad, el ciberterrorismo se refiere al uso de Internet para atacar infraestructuras críticas con la intención de provocar miedo y causar daños físicos a las personas (heridas graves o la muerte), para que tenga un efecto en el cambio de gobierno o en la misma población en base a metas políticas, o ideológicas. Así se pone de manifiesto la complejidad del fenómeno que nos lleva a la idea de indefinición del ciberterrorismo, al menos, en el plano científico.

En resumen y para poder entender esta indefinición de terrorismo, podemos decir que existen dos tipos de acciones ciberterroristas: por un lado, el ciberterrorismo puro, en el que se busca causar un daño única y exclusivamente con medios cibernéticos, e incluso, tecnológicos; y, por otro lado ,las acciones de

apoyo al terrorismo tradicional a través de actos de ciberterrorismo réplica (financiación, reclutamiento, intercomunicación, formación y difusión de acciones).

Una vez vistos los problemas de definición y los elementos que componen dicha definición, cabe preguntarnos por la intersección con otras tipologías criminológicas para avanzar en su conocimiento: ciberguerra y ciberhackivismo. Una primera aproximación a lo que es la ciberguerra proviene de Miró (2012: 301), en la que indica que "son actos de guerra entre Estados o contra Estados en el ciberespacio". Aunque también se trata de una definición simplista, como lo visto para el ciberterrorismo, ya que no es sencillo definir lo que es la ciberguerra, entre otras cuestiones, porque en el ciberespacio no operan las mismas leyes que en el espacio físico tradicional y, por tanto, tampoco las relacionadas con las leyes de guerra tradicional. Aunque hay más intentos de definición del problema, como el de Brenner (2008, citado en Holt, Boosler y Seigfried-Spellar, 2015) como "operaciones militares por medios virtuales que tienen los mismos fines que se persiguen con el uso de fuerzas militares convencionales". Y aquí nos lleva al término de ciberarmas, importantes ya que no solo se usan las ciberfuerzas militares para la defensa, sino también para el ataque a través de nuevas armas que actúan en el ciberespacio.

Para diferenciar los actos de ciberguerra de los de ciberterrorismo, podemos tener en cuenta lo que nos indica Maras (2017: 391) en cuanto a la atribución de los ciberataques. De esta manera, no podemos considerar un ciberataque como acto de ciberguerra si no hay una atribución de un país; por lo que puede suceder lo mismo sin la atribución de responsabilidad de un grupo terrorista no estaremos hablando de ciberterrorismo.

En cuanto al ciberhackivismo, es entendido como "el conjunto de ataques llevados a cabo por hackers informáticos, pero sin una intención maliciosa de defraudar a las víctimas, de robarles información para traficar con ella o de causar daños para perjudicar económicamente, sino con la intención de mandar un mensaje ideológico, de lucha política, y defensa de ideas, generalmente relacionadas con la libertad de Internet, aunque pueden tener cabida cualesquiera otras convenciones ideológicas" (Miró, 2012: 301-302). De nuevo esta definición nos deja dudas en cuanto a las diferencias con el ciberterrorismo, ya que si partimos de esta premisa, encontramos semejanzas en torno a la motivación ideológica y esto nos lleva de nuevo a establecer la diferencia entre ciberhackivisto y ciberterrorismo en cuanto al grupo que se encuentre detrás de la atribución de los ciberataques.

A este respecto cabe preguntarnos si la injerencia parece ser de países como Rusia, en el plano de la soberanía nacional española en Cataluña, y si puede atribuirse a un acto de ciberguerra, ciberhackivismo o ciberterrorismo. En este sentido en España se está investigando por parte de la Audiencia Nacional la posible injerencia de servicios secretos rusos en el denominado "proces" de independencia de la región española de Cataluña (López-Fonseca y Pérez, 2019).

Como hemos podido comprobar, la definición de ciberterrorismo no es sencilla y tampoco lo es en cuanto a la diferencia con otros fenómenos que se pueden incluir dentro de los ciberataques políticos (ciberguerra y ciberhackivismo). La clave para la definición y diferenciación estará en la atribución de los ciberataques y las personas o los grupos que puedan estar tras ellos.

Avancemos un poco más para aportar algo de luz en cuanto a la evolución del ciberterrorismo y las diferentes capacidades de respuesta preventiva frente a ellas, y así trataremos de comprobar la hipótesis inicial de esta investigación: "Las capacidades de defensa y seguridad españolas, como país miembro de la Comunidad Internacional, hacen que esté preparada para hacer frente a la amenaza futura ciberterrorista".

2.Un poco de historia, ¿cómo hemos llegado a la situación actual?

Si obviamos toda la historia del terrorismo desde sus inicios y nos situamos a partir de los años 1990 en España, por el inicio del uso masivo de Internet, podemos comprobar que existen dos periodos de actividad protagonizados por dos grupos diferentes (ETA y Daesh). Ambos períodos de actividad coinciden de manera

casi perfecta con la descripción de las dos últimas olas del terrorismo moderno de Rapoport (2002): de 'nueva izquierda' y el 'religioso'.

En los 90, mientras la población civil mundial (especialmente en Occidente) se comenzaba a acostumbrar al uso de Internet, sobre todo la web, ya era noticia el uso por parte de la banda terrorista ETA de servidores informáticos en el extranjero para difundir su visión del que llamaban "conflicto vasco", tratando de eludir así la infracción de la legislación española contra apología terrorista (Europa Press, 1997). La hemeroteca sí permite vislumbrar, no obstante, que esa actividad terrorista en Internet fue provechosa para la banda que el aparato etarra pudo conseguir, la que integraba intercambios logísticos y de know-how de la organización vasca con el terrorismo de "nueva izquierda" internacionaizado (Rapoport, 2002).

El anonimato inicial y uso personal de las redes sociales sí parece provocar una actividad algo más profusa en favor de la imagen histórica de ETA. Es más habitual encontrar ahí opiniones que defendían la lucha armada de la banda e incluso ofendían a las víctimas. En esos casos, de manera general, la ley actúa, por ejemplo, en abril de 2014: la Guardia Civil juntó varios de estos expedientes en la primera fase de la Operación Araña, que se saldó con 21 detenidos de entre 16 y 53 años. Eran responsables de publicar en Twitter y Facebook mensajes como (Escrivá y Lázaro, 2014):

> "Vuestros muertos son nuestra alegría y nuestra diversión"
>
> "Lástima que ya no haya ETA para que seas la nueva Irene Villa"
>
> "Gora ETA, muerte el Partido Popular y larga vida al terrorismo el asesinato y la extorsión de políticos, guardias civiles y policías"
>
> "Lo mejor que nos podría ocurrir es la vuelta de ETA a las armas y posterior eliminación del Partido Popular a base de bombas y tiros en la nuca",
>
> "Me la suda por tiempos la muerte de Miguel Ángel Blanco. Es más, me alegro más ahora porque deseo la vuelta de ETA para que haga lo mismo"
>
> "El próximo 13 de mayo sería el cumpleaños de Miguel Ángel Blanco, pero oooh ETA le metió dos tiros en la chola #quesejoda #pudrete"

Entre 2014 y 2016 esta operación tuvo 4 fases y acabó con 76 detenidos. Lo publicado iba "desde el ensalzamiento de diversas organizaciones terroristas, hasta la burla hacia víctimas concretas del terrorismo", según informó en su día la Guardia Civil (2016).

Si nos centramos en el segundo grupo con amplia influencia en España, Daesh, el estudio de su estrategia mediática ha sido ampliamente estudiada en sectores académicos, que muestran que se basa en imágenes de alto impacto y cuidados rodajes y ediciones audiovisuales, a través del uso no sólo de la web sino también de las redes sociales, y aprovecha la curva ascendente de las principales plataformas (Cano Paños, 2019, Cano Paños y Castro Toledo, 2018; Torres Soriano (2009) o Ministerio de Defensa, 2014) y recogida en los medios de comunicación.

De hecho, mientras que antecesores como Al Qaeda y organizaciones que pudieran considerarse afines relegaban su labor comunicativa externa a revistas (en formato digital o incluso en papel) y apariciones de sus líderes con monótonos planos fijos, aunque la intervención durase varios minutos, Daesh convirtió sus elaborados y aterradores mensajes audiovisuales en una pata más de su actividad, a partir de su diseminación en Internet y las redes sociales, difundiéndolos y protegiéndolos de los esfuerzos oficiales por borrarlos, especialmente en Twitter.

Hoy, por su parte, el mal llamado 'cibercalifato' o 'califato 2.0' continúa su labor comunicacional en las redes sociales, aunque se centre fundamentalmente en el recluta-miento y difusión de su visión wahabista/yihadista del Islam, toda vez que, al mismo tiempo, permanecen y se incrementan los filtros y eliminación de perfiles asociados con ese tipo de propaganda (en colaboración de las autoridades contraterroristas con las empresas propietarias de las plataformas sociales). Cabe destacar que estas acciones se consideran ilegales en la mayor parte de países de Occidente. Por ello las posibilidades de publicación hacia el gran público se ha visto mermada. No obstante, sigue siendo real y patente la relación descrita entre el ciberterrorismo y la comunicación "El terrorismo moderno es un fenómeno de comunicación. Una táctica extrema, criminal

y violenta. empleada para marcar la agenda de los medios y captar la atención de la opinión pública hacia una determinada reivindicación política" (Lesaca Esquiroz, 2017). Y aquí queda patente la importancia del ciberespacio en cuanto a la evolución de la amenaza ciberterrorista, sobre todo en lo que son actos de ciberterrorismo réplica, como indicamos en el punto anterior.

3.Capacidades prospectivas españolas

La primera aclaración que debemos hacer aquí es por qué se denominan capacidades prospectivas. Se debe a que la prospectiva, como herramienta de metodología y en el campo de los estudios de futuro, trata de predecir el futuro desde una perspectiva holística, proactiva y anticipatoria (Bas, 1999: 12). Por este motivo denominamos a las capacidades que se presentan a continuación como prospectivas, ya que todas ellas tratan de "predecir" el futuro, sobre todo en su vertiente preventiva.

Además, otra de las características prospectivas de la lucha contra el ciberterrorismo se incluye en la Estrategia Nacional de Seguridad española (2017) vigente. Esta estrategia establece, ya desde su título, una respuesta primaria al cambio de paradigma moderno en los desafíos a la seguridad ("un proyecto compartido de todos y para todos"): que prevenir, advertir y denunciar vectores de riesgo y ataque a la seguridad de los españoles, así como la potenciación de la resiliencia y el trabajo de normalización tras una brecha más o menos importante de seguridad, no puede ser ya, para ser efectivos, una tarea exclusivamente de las administraciones públicas; esta responsabilidad debe alcanzar a los ciudadanos. Esa filosofía (heredada de la anterior estrategia nacional de 2013), se concreta en sentencias dentro de su texto como que "una Seguridad Nacional eficaz requiere tanto la sensibilización social de los ciudadanos como la participación de sus representantes" (DSN, 2017: 26) o: "Una sociedad conocedora de las amenazas y desafíos para la seguridad es una sociedad mejor preparada y con mayor capacidad de sobreponerse ante las crisis a las que tenga que enfrentarse. Una sociedad concienciada es pues, más segura, robusta y resiliente. Ello implica la participación ciudadana como uno de los ejes de actuación sobre los que descansa la verdadera efectividad de esta política pública" (DSN, 2017: 83).

La participación ciudadana aparece como tanto más importante en cuanto se refiere a ámbitos que pudieran considerarse íntimos o privados de la seguridad, como los dispositivos electrónicos personales, donde, en el caso que nos ocupa para este trabajo, un nacional puede detectar actividad terrorista sin necesidad de dedicarse profesionalmente a ello o ser un agente de la autoridad.

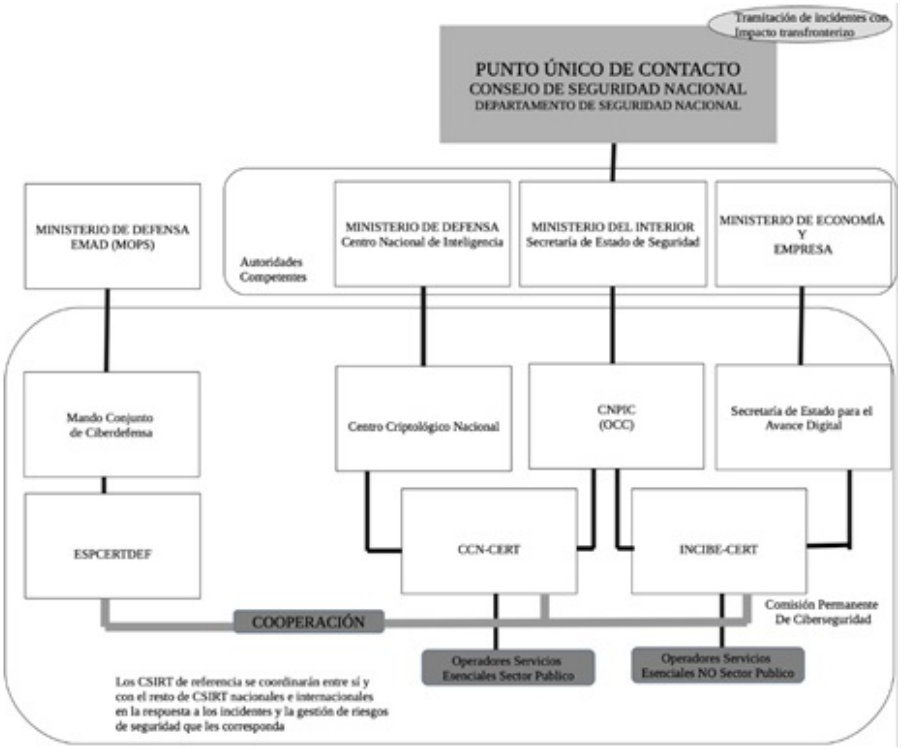

FIGURA 1
Actores en la ciberseguridad nacional (España)
Fuente: CCN-CERT (2018)

No obstante, y en línea con el documento estratégico marco mencionado (que destaca la colaboración privada, pero reafirma la titularidad de la responsabilidad de la seguridad nacional al aparato del Estado), España se ha dotado de un completo ecosistema oficial de lucha contra las ciberamenazas (figura 1). Debemos señalar que cada elemento de este engranaje público puede tener participación en caso de ciberterrorismo.

Puestos a categorizarlos, a nivel estatal encontramos cuatro tipos de agentes con atribuciones contraciberterroristas de acuerdo con su naturaleza y objetivos señalados por la legislación aplicable en cada caso:

1. Coordinación, acción y estudio: El Departamento de Seguridad Nacional, adscrito al gabinete del Presidente del Gobierno, y el Centro Criptológico Nacional, perteneciente al CNI, dependiente del Ministerio de Defensa.
2. Policiales: la Unidad de Investigación Tecnológica del Cuerpo Nacional de Policía, el Grupo de Delitos Telemáticos de la Guardia Civil y el Centro Nacional de Protección de Infraestructuras y Ciberseguridad de la Secretaría de Estado de Seguridad.
3. Civil y empresarial: el INCIBE (Instituto Nacional de Ciberseguridad, antes Instituto Nacional de Tecnologías de la Comunicación).
4. Militar: Mando Conjunto de Ciberdefensa

Describiremos a continuación sus atribuciones y características, así como algunas de sus actuaciones más destacadas en el ámbito del ciberterrorismo:

I. Capacidades gubernamentales y de coordinación en España

En esta categoría los dos organismos integrantes pertenecen directamente al Gobierno de la nación. En primer lugar está el Departamento de Seguridad Nacional (DSN), dependiente orgánicamente del gabinete del Presidente del Gobierno (Real Decreto 1119/2012 de 20 de julio, de modificación del Real Decreto 83/2012, de 13 de enero, por el que se reestructura la Presidencia del Gobierno). Dentro de su organigrama (figura 2), una unidad específica está encargada de eventualidades ciberterroristas, la de 'ciberseguridad y desinformación'.

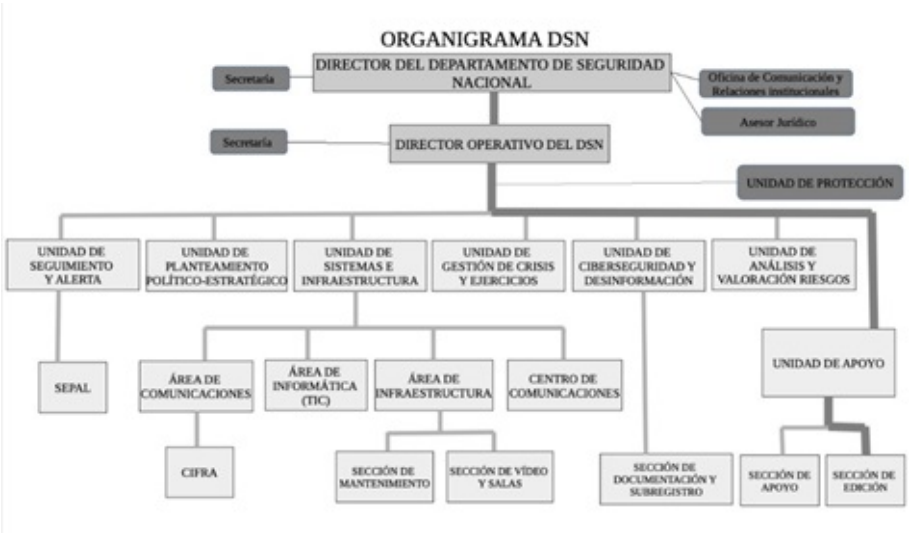

FIGURA 2
Organigrama del DSN
Fuente: Departamento de Seguridad Nacional

Por ley 36/2015, de 28 de septiembre, el DSN tiene asignadas cuatro funciones principales:

- Secretariado técnico del más alto órgano colegiado de trabajo del Gobierno en materia de Seguridad Nacional, el Consejo de Seguridad Nacional.
- En relación con lo anterior, desempeña funciones de secretariado técnico también para las comisiones interministeriales relacionadas con la Seguridad Nacional (SN) que a su vez surten de material de trabajo al Consejo.
- Gestión de crisis
- Apoyo a la colaboración y correcto funcionamiento de los órganos públicos estatales dedicados a la SN y realización de propuestas para fomentar la participación privada en la materia

Cada una de estas funciones podría facultar al DSN a intervenir en procesos de deliberación y toma de decisiones en caso de ataque ciberterrorista a intereses nacionales. Su participación, por las características del órgano, es de preparación (incluida la labor de difusión de cultura de seguridad hacia la sociedad), respuesta inmediata (dado, por ejemplo, un ataque ciberterrorista sostenido en el tiempo o para coordinar la respuesta necesaria a un ciberataque terrorista puntual pero de cierta magnitud) y no inmediata y forense. Es decir: abarca todo el abanico temporal de lucha contraciberterrorista desde el punto de vista gubernamental.

La segunda de sus funciones es la de asistencia (además de al Consejo Nacional de Seguridad Marítima, Comité de Situación para la gestión de crisis, Comité Especializado de Inmigración, Comité Especializado de No Proliferación y Comité Especializado de Seguridad Energética) al Consejo Nacional de Ciberseguridad (CNC) (figura 3).

FIGURA 3
Composición del Consejo Nacional de Ciberseguridad
Fuente: DSN

El CNC es un órgano (creado por acuerdo del Consejo de Seguridad Nacional el 5 de diciembre de 2013) de encuentro del DSN con el segundo organismo integrante de esta categoría de actores públicos nacionales con atribuciones de coordinación, acción y estudio: el Centro Nacional de Inteligencia (CNI), vía su rama cibernética: el Centro Criptológico Nacional (CCN).

El principal órgano de Inteligencia del Gobierno de España, el CNI, ha sido a lo largo de su historia dependiente o bien del Ministerio de Defensa o bien del de Presidencia. El cumplimiento de las directrices gubernamentales de Inteligencia se ha venido entendiendo en las últimas décadas de manera más puramente política o militar según la visión del Gobierno de turno o su conveniencia. Así, el Servicio Central de Documentación (SECED, 1972-1977) nació adscrito al Ministro Subsecretario de Presidencia, Almirante Luis Carrero Blanco. Con la llegada de la democracia, tomó el relevo el Centro Superior de Estudios de la Defensa (CESID, 1977-2002) con la renovada misión de surtir de información a la Defensa Nacional de la España democrática. Ya en 1984 (tras la llegada del Partido Socialista Obrero Español –PSOE– al poder) hubo un primer cambio, un nuevo Real Decreto convertía a los servicios de inteligencia en una herramienta de uso mixto entre Presidencia y Defensa.

El 6 de mayo de 2002 es aprobada la Ley 11/2002, reguladora del Centro Nacional de Inteligencia con la que nace el CNI y que en su artículo 7 lo hace depender del Ministerio de Defensa. Así ha sido salvo en el período 2011-2018 en el que los Gobiernos correspondientes lo creyeron mejor incardinado de nuevo en el Ministerio de Presidencia (con la misma titular que la Vicepresidencia en esas legislaturas, Soraya Saenz de Santamaría, del Partido Popular). En 2018, el PSOE le devolvió a su dependencia orgánica de Defensa.

Al margen de ese contexto histórico, del que es no obstante deudora, su rama cibernética, el CCN, desarrolla en la actualidad una múltiple labor de CERT (Computer Emergency Response Team) público nacional, asistiendo y colaborando con organismos públicos y empresas de interés estratégico frente a ciberataques y su posibilidad. Según la web del organismo, el CCN tiene como misión "contribuir a la mejora de la ciberseguridad española, siendo el centro de alerta y respuesta nacional que coopere y ayude a responder de forma rápida y eficiente a los ciberataques y a afrontar de forma activa las ciberamenazas, incluyendo la coordinación a nivel público estatal de las distintas Capacidades de Respuesta a Incidentes o Centros de Operaciones de Ciberseguridad existentes" (CCN-CERT, 2019).

Concreta estos objetivos con una importante producción de material divulgativo público, la colaboración en la resolución y prevención de incidentes (ataques o creación de riesgos de seguridad) con sus sectores objetivo antes mencionados de manera confidencial y el asesoramiento del Gabinete gubernamental, especialmente a través del mencionado Consejo Nacional de Ciberseguridad, en el que coincide con el DSN.

En cuanto a lo que se puede analizar de sus atribuciones contraciberterroristas, el propio CCN afirma que, de acuerdo con la Ley 11/2002 de creación del CNI y la 40/2015 de Régimen Jurídico del Sector Público, es su competencia "la gestión de ciberincidentes que afecten a cualquier organismo o empresa pública. En el caso de operadores críticos del sector público la gestión de ciberincidentes se realizará por el CCN-CERT en coordinación con el CNPIC" (CCN-CERT, 2019)

Se puede concluir por tanto que, al margen de su labor de divulgación pública, las atribuciones legales del CCN en materia de asesoramiento gubernamental, lo habilitan para proveer a los órganos de decisión superiores de información y análisis técnico en materia anticiberterrorista, llegado el caso.

II. Capacidades policiales en España.

Como en muchos otros países, en España las contramedidas contra el quebrantamiento de la ley y el orden, en el ciberespacio y desde él, tienen una primaria faceta policial, esto es, de lucha y prevención del delito a través de medios digitales. Desde hace años, la capacitación de efectivos policiales en este ámbito (en el entorno estatal pero también en los casos de las policías de las Comunidades Autónomas que disponen de ellas: País Vasco, Navarra, Cataluña e Islas Canarias) les ha convertido en fuerzas que podrían intervenir en supuestos de ataques ciberterroristas; de hecho tienen un papel muy activo en operaciones contra el proselitismo terrorista en Internet y aún mucho más en la detección, investigación y acción contra delincuentes y delincuencia organizada en la Red o que usan Internet para conseguir sus fines.

Al margen de labores de información y físicas por proximidad, las policías autonómicas no juegan un papel importante en la actualidad en España en el control del ciberdelito. Esto es así a pesar de que toda la legislación estatal y autonómica les atribuye lógicas funciones de mantenimiento del orden y lucha contra la criminalidad, si bien en la práctica, en el terreno cibernético, la autoría de las actuaciones policiales en este ámbito en el país pertenece a quienes sí están dotados de medios y personal adiestrado para ello: la Policía Nacional y la Guardia Civil. Serán, junto con el Centro Nacional de Protección de Infraestructuras Críticas (CNPIC), los actores que trataremos en este epígrafe.

El Cuerpo Nacional de Policía (CNP) o Policía Nacional tiene encargada la vigilancia del ciberespacio dentro de sus competencias a su Brigada de Investigación Tecnológica (lo que le dota de unas distintivas y oportunas siglas, 'BIT'), encuadrada dentro del la Unidad de Investigación Tecnológica de la Comisaria General de Policía Judicial de la Dirección General de la Policía (DGP). El dibujo de ese organigrama ya otorga idea del marco de sus funciones y es una plasmación de lo que, por otro lado, ordena la legislación apuntada: atención y prevención del quebrantamiento del orden legal en el ciberespacio en este caso, así como su investigación e intervención en contra, bajo supervisión judicial. En palabras de la DGP, "la Brigada Central de Investigación Tecnológica es la Unidad policial destinada a responder a los retos que plantean las nuevas formas de delincuencia. Pornografía infantil, estafas y fraudes por Internet, fraudes en el uso de las comunicaciones, ataques cibernéticos, piratería" (UDEF, 2019).

Específicamente, la Policía Nacional cita los siguientes supuestos delictivos entre las competencias de la Brigada Central de IT (UDEF, 2019):

- Amenazas, injurias, calumnias. Por correo electrónico, SMS, tablones de anuncios, foros, newsgroups, web...
- Pornografía infantil. Protección al menor en el uso de las nuevas tecnologías.
- Fraudes en el uso de las comunicaciones. Piratería de señales de televisión privada

- Fraudes en Internet. Estafas. Uso fraudulento de tarjetas de crédito. Fraudes en subastas. Comercio electrónico
- Seguridad lógica. Virus. Ataques de denegación de servicio. Sustracción de datos. Hacking. Descubrimiento y revelación de secreto. Suplantación de personalidad. Sustracción de cuentas de correo electrónico.
- Piratería de programas de ordenador, de música y de productos cinematográficos.

Varios de esos supuestos pueden suponer bien parte de una táctica terrorista, bien una actividad ilícita convencional relacionada con el terrorismo (como lo puede ser la apología terrorista), bien un ataque de esa misma naturaleza y origen en sí mismo.

Dependiendo de la magnitud de los hechos ante los que se encuentren los agentes y su potencialidad, el caso puede ser neutralizado policialmente de manera habitual o elevado a instancias superiores, hasta alcanzar la intervención del Departamento de Seguridad Nacional y el Consejo de Seguridad Nacional. Es necesario tomar en consideración que las labores de vigilancia habituales de los agentes y oficiales encargados, la recepción de denuncias e informaciones, así como las alianzas internacionales y los datos e indicios que se puedan recabar gracias a ellas, pueden hacerles hallar rastros de delito en el ciberespacio cuyas dimensiones y posibles implicaciones obliguen a un escalado del asunto a instancias superiores. Lo contenido en el presente párrafo es igualmente válido para el siguiente cuerpo a analizar.

La Guardia Civil crea su Grupo de Delitos Informáticos en el seno de su Unidad Central Operativa en 1996. En la actualidad se denomina Grupo de Delitos Telemáticos (GDT). Define el ámbito de sus competencias así:

> Con la socialización de Internet y el crecimiento de los hechos delictivos, se amplía el abanico de competencias de investigación, que alcanza a todas aquellas conductas delictivas realizadas a través de los sistemas de información o contra éstos, lo que se conoce popularmente como el cibercrimen. (...) El esfuerzo principal del GDT y de los EDITEs ha sido, desde su creación, la investigación de la delincuencia que se vale de las redes y sistemas de información para su comisión (Guardia Civil, 2019)

Al igual que sucede con el CNP, los agentes destinados en el GDT pueden toparse con conductas constitutivas de delitos relacionados con el terrorismo en el ciberespacio. De hecho, como hemos recogido anteriormente, la Guardia Civil ha tenido un papel fundamental en la persecución y represión de la apología del terrorismo de ETA en España tras la caída de la banda. Del mismo modo, en la actualidad y al igual que la Policía Nacional, sus actuaciones de investigación en redes sociales, foros privados y espacios de la dark web dan lugar a operaciones que concluyen con la detención de sujetos afines a la principal amenaza terrorista en la actualidad para España, el de etiología yihadista.

Para finalizar este apartado, cabe mencionar el Centro Nacional de Protección de Infraestructuras y Ciberseguridad (CNPIC), es un órgano de respuesta y coordinación a nivel policial para la protección de infraestructuras críticas, en teoría, principal objetivo del ciberterrorismo. Según se recoge en su web (CNPIC, 2020),

> el Centro Nacional de Protección de Infraestructuras y Ciberseguridad (CNPIC) es el órgano responsable del impulso, coordinación y supervisión de todas las políticas y actividades relacionadas con la protección de las infraestructuras críticas españolas y con la ciberseguridad en el seno del Ministerio del Interior. El CNPIC depende del Secretario de Estado de Seguridad, máximo responsable del Sistema Nacional de Protección de las Infraestructuras Críticas y de las políticas de ciberseguridad del Ministerio.

III. Capacidades civiles y empresariales.

Dentro del repaso a los distintos actores anti ciberterroristas categorizados, acabamos con el INCIBE, con sede en León. Según su propia página web (INCIBE, 2019):

el Instituto Nacional de Ciberseguridad de España (INCIBE), anteriormente Instituto Nacional de Tecnologías de la Comunicación, es una sociedad dependiente del Ministerio de Economía y Empresa a través de la Secretaría de Estado para el Avance Digital y consolidada como entidad de referencia para el desarrollo de la ciberseguridad y de la confianza digital de ciudadanos, red académica y de investigación, profesionales, empresas y especialmente para sectores estratégicos.

Para llevar a cabo esta misión, el INCIBE ejecuta una serie de tareas, entre las que destaca (por ser la orientada a alcanzar al mayor número de población) la Oficina de Información al Internauta (OSI), que proporciona información básica e intermedia a todo tipo de usuario de Internet vía formulario web, realizando campañas periódicas de concienciación de los distintos riesgos digitales o con un consultorio telefónico, la Línea de Ayuda en Ciberseguridad. El Gobierno de la nación, en octubre de 2019, concedía a este último servicio de la OSI un carácter aún más institucional, al adjudicarle el número corto de contacto 017. Esta línea supone uno de las líneas de acción más visibles de la OSI del INCIBE, que dedica especial atención a colectivos digitales especialmente vulnerables como niños (con el programa/web 'Internet segura for kids') o novatos en la Red.

El INCIBE también atiende las necesidades de información y ayuda a planificación en materia de ciberseguridad de empresas, organizaciones e instituciones. A su vez, supone un centro de estudio de amenazas digitales, que concreta en varias publicaciones como sus 'Balances de Ciberseguridad', editados anualmente.

Por último, es un centro de coordinación de actores clave a su vez a nivel nacional e internacional en materia de ciberriesgos, con los que intercambia información y coordina acciones. De hecho, en ese sentido, en enero de 2020 fue nombrado Autoridad de Numeración de Vulnerabilidades (CNA: CVE Numbering Authorities) por Mitre, una asociación dependiente del National Institute of Standards and Technologys del Departamento de Comercio de Estados Unidos; eso supone que el INCIBE es el único organismo español válido para la interlocución con ese organismo americano para la comunicación de la detección de vulnerabilidades en equipos y sistemas TIC.

Su naturaleza hace que el INCIBE tenga una inclinación de ciberseguridad más ciudadana y empresarial, orientada a los riesgos del día a día, no tanto al ciberterrorismo. No obstante, con los distintos canales que tiene abiertos con sus interlocutores puede recibir información relacionada directa o indirectamente con actividad ciberterrorista que pondrá en conocimiento de las fuerzas nacionales directamente encargados de su lucha y prevención (por ejemplo, comunicaciones de empresas informando de que han sufrido un ataque de naturaleza terrorista o ciudadanos informando de que han presenciado propaganda terrorista en Internet).

IV. Capacidades militares.

El mando conjunto de ciberdefensa en España fue creado por la Orden Ministerial de 10/2013, del 19 de febrero, y está subordinado al Jefe del Estado Mayor de la Defensa (JEMAD). Las siguientes misiones han sido encomendadas (EMAD, 2020) a él:

- Garantizar el libre acceso al ciberespacio, con el fin de cumplir las misiones y cometidos asignados a las Fuerzas Armadas, mediante el desarrollo y empleo de los medios y procedimientos necesarios.
- Garantizar la disponibilidad, integridad y confidencialidad de la información, así como la integridad y disponibilidad de las redes y sistemas que la manejan y tenga encomendados.
- Garantizar el funcionamiento de los servicios críticos de los sistemas de información y telecomunicaciones de las Fuerzas Armadas en un ambiente degradado debido a incidentes, accidentes o ataques.
- Obtener, analizar y explotar la información sobre ciberataques e incidentes en las redes y sistemas de su responsabilidad.
- Ejercer la respuesta oportuna, legítima y proporcionada en el ciberespacio ante amenazas o agresiones que puedan afectar a la Defensa Nacional.
- Dirigir y coordinar, en materia de Ciberdefensa, la actividad de los centros de respuesta a incidentes de seguridad de la información de los Ejércitos y Armada y el de operaciones de seguridad de la información del Ministerio de Defensa.
- Cooperar, en materia de ciberdefensa, con los centros nacionales de respuesta a incidentes de seguridad de la información, de acuerdo con lo que determinen las estrategias y políticas nacionales de ciberseguridad en vigor, así como con otros centros militares de respuesta a incidentes de seguridad de la información en el ámbito internacional.

- Definir, dirigir y coordinar la concienciación, la formación y el adiestramiento especializado en materia de ciberdefensa.

Como podemos observar tiene dos cometidos diferenciados: por un lado, la protección de la información de las unidades dependientes de Defensa y, por otro, los cometidos de respuesta a incidentes. También los cometidos de coordinación son sumamente importantes en estas tareas, ya sea a nivel interno, con centros de los diferentes ejércitos, a nivel nacional (centros nacionales, policiales o civiles) o a nivel internacional. Y aquí es donde entroncamos con la colaboración a nivel OTAN.

En este sentido la Organización del Tratado del Atlántico Norte (OTAN o NATO, por sus siglas en inglés) está preocupada por el ámbito de las ciberamenzas, como pone de manifiesto a través de su web (OTAN, 2020). Y aquí es donde encontramos el objetivo principal que persigue en la ciberdefensa, el cual no es otro que el fortalecimiento de las infraestructuras nacionales y las redes. Para ello cuenta con más de 200 profesionales que realizan análisis diarios, dos equipos de reacción rápida para asistir a los aliados, un simulador de ciberjercicios, proyectos de inteligencia de defensa (Smart Defense) y el Centro de Excelencia en Ciberdefensa de Tallin.

Debemos detenernos en este centro, porque es uno de los lugares importantes de colaboración, aparte de un acuerdo técnico con la Unión Europea, más de cuarenta acuerdos con los países socios y más de quince con empresas tecnológicas. Bien, este centro de excelencia realiza investigación, entrenamiento y análisis en cuatro áreas: tecnología, estrategia, operaciones y leyes (CCDCOE, 2020).

Otro aspecto de interés en el marco OTAN es el Programa de Seguridad y Paz. A través de este programa se ha provisto de investigación de interés en el ámbito del ciberterrorismo, por ejemplo, en 2008 la publicación de *Responses to Cyberterrorism* ,que recoge 11 trabajos en las áreas de historia de Internet, sistemas abiertos de inteligencia, infraestructuras críticas, uso de Internet por los terroristas, colaboración internacional, AlQaeda web, Internet como herramienta contraterrorista, Análisis del PKK/KRONGRA-GEL o el papel de la OTAN en el ciberterrorismo (Center of Excellence Defense Against Terrorism, 2008). O la publicación más actual de 2015 sobre *Terrorist Use of Cyberspace and Cyber Terrorism: new challenges and responses*, donde se reflejan 15 trabajos en áreas relativas al uso de la tecnología por ciberterroristas y ciberdelincuentes, terrorismo global, protección de información crítica, financiación del terrorismo, Al Qaeda, ISIS, el factor humano en el ciberterrorismo, propaganda terrorista en el ciberespacio, legislación antiterrorista, legislación internacional y legislación italiana, y respuestas al ciberterrorismo (Ogun, 2015).

4.Conclusiones para el futuro.

Como hemos expuesto, para activar los mecanismos que deben hacer frente a una ciberamenaza conviene determinar qué tipo de ciberamenaza es y, sobre todo, cuál es la intencionalidad. Este aspecto, en el ámbito de este trabajo, el ciberterrorismo, nos lleva a algo más complejo como es determinar quién es ciberterrorista. Esta aparente indefinición, o el que no exista una clara definición en el campo académico, cuenta con dos pilares básicos: la falta de casos reales y el problema ideológico.

En primer lugar, para el análisis de escenarios probables, el hecho de que nos hallemos ante un fenómeno no ya nuevo, sino que seguramente ha echado a andar por ahora mucho más en la ficción que en la realidad, no ayuda a clarificar la cuestión. En cambio, no existe por ahora una actividad terrorista per se permanente ni especialmente intensa en el ciberespacio más allá del potente desarrollo proselitista, apologético y promocional en redes sociales y canales semipúblicos de servicios de mensajería de organizaciones terroristas (ej. Daesh) e ideales (supremacía blanca) bien implantados. El propio Candau, citado ya al principio de este trabajo, niega haber visto algún caso aún de ciberataque terrorista ("será cosa de que mañana tengamos un caso, pero hoy por hoy no ha habido ninguno") (Congreso de los Diputados, 2018) y la práctica totalidad

de las fuentes académicas corroboran que aún no se ha sufrido (o al menos no ha sido conocido) ninguno a media o gran escala.

Hay autores que, no obstante lo dicho, sí señalan la comisión de actos ciberterroristas, por ejemplo, a finales de los años 90 por parte de Hezbollah y Hamas (deben tomarse siempre, ante la falta de reconocimiento oficial, con la previa y necesaria etiqueta de "presuntos") (Pettinari, 1997: 7-8). Y es que, en la relación de pros y contras de atacar como terrorista en el ciberespacio salen ganando las contras; ante la facilidad de ejecución, menor coste económico o deslocalización geográfica hay que contraponer la dificultad para provocar grandes catástrofes o aumento de la conciencia social y política sobre ciberseguridad entre los segundos, a lo que debe añadirse la posibilidad de negación de la existencia del ataque por parte de las autoridades o entidades afectadas si éste no alcanza un nivel de gravedad tal que lo ponga en conocimiento público de manera automática.

Si ahondamos en esta idea, aunque hace 30 años –década de los 70– la visión del National Research Council indicaba que "el terrorista del mañana podrá hacer más daño con un teclado que con una bomba" (citado en Denning, 2001), ya Denning (2001) dejó constancia de una realidad tras el 11-S que aún hoy sigue vigente: "Al menos por ahora, los vehículos robados, camiones bomba y armas biológicas parecen suponer una amenaza mayor que el ciberterrorismo. No obstante, tal y como los sucesos del 11 de septiembre nos cogieron por sorpresa, así podría a pasar con un gran ciberataque. No podemos permitirnos descartar la amenaza". En este sentido también se expresa Nieto (2018) y afirma que no actualmente es ficción un ataque ciberterrorista a infraestructuras críticas, aunque el futuro sea impredecible, porque los grupos terroristas no disponen de tecnología suficiente y remarca que lo más factible sea la influencia en audiencias concretas, más que ciberataques a estas infraestructuras.

Tampoco ayuda a la clarificación de la situación el uso que hacen de manera general los medios de comunicación de los términos 'cibercrimen', 'ciberataque', 'ciberdelincuencia', el propio de 'ciberterrorismo' u otros más especializados como 'hacktivismo'. Son empleados en muchas ocasiones como sinónimos sin atender a los matices o grandes diferencias entre unos y otros.

En segundo lugar, el problema de indefinición que arrastra el ciberterrorismo lo hereda de su matriz terminológica, condensada en la expresión "un terrorista para alguien es un luchador por la libertad para otro". Como indica Jenkins (1982), "[l]a dificultad de definir el terrorismo ha llevado al cliché de que un terrorista para alguien es un luchador por la libertad para otro, lo que implica que no puede haber una definición objetiva de terrorismo, ni estándares universales de comportamiento en la paz o la guerra".

Otro de los aspectos relacionados de la indefinición del concepto tiene que ver con los problemas relacionados con la confusión de actos de ciberguerra o de actos de ciberhackivismo, como se ha comprobado, en los que la determinación vendrá dada por los intereses de los grupos que estén detrás de los ciberataques. Por eso es muy importante la investigación del factor humano y de la toma de decisiones en este campo y así poder determinar la tipología frente a la que nos encontramos y activar unas capacidades u otras, tanto a nivel nacional como internacional.

Así, estamos listos para detectar los ataques del ciberterrorismo, un problema aún de futuro, allá cuando se produzcan: acciones cibernéticas que, con o sin efectos físicos en el mundo real, busquen atemorizar a una población o parte de ella, con el fin de acercar, conseguir o promocionar los fines ideológicos del ente personal o colectivo que las perpetra. Se trata, por tanto, del uso de tácticas cibernéticas por parte del terrorismo, si bien aún el mundo no ha visto una actividad prolija en ese campo, más allá del proselitismo volcado en redes sociales, foros y dark web.

Una de las primeras conclusiones es que el escenario de futuro más probable no es el de una acción terrorista directa a través de un ciberataque de gran impacto, sino más bien la potenciación de la propaganda, captación, adiestramiento y comunicación de grupos terroristas.

En abundamiento de lo expuesto, hemos de emplear lo anteriormente expuesto para dejar sentada una clara doble base que se afianza tras analizar la historia del ciberterrorismo en España: en primer lugar,

como atestiguan el jefe de ciberseguridad del CCN, Javier Candau (Congreso de los Diputados, 2018), y los informes públicos que viene emitiendo este organismo, aún no ha existido un ataque ciberterrorista en España (CCN-CERT, 2018, 2019); en segundo lugar, y relacionado con lo anterior, la actividad terrorista en el ciberespacio de dominio español (presencia de ciudadanos españoles) se limita hasta ahora al ámbito propagandístico, apologético, proselitista, financiador y/o reclutador de la ideología terrorista de turno.

Aunque, por otra parte, la evolución desde 2017, en la que las publicaciones cibernéticas favorables a los intereses de la organización terrorista internacional deben ser, más que nunca, buscadas para poder ser leídas y, por ello, su actividad se ha trasladado a foros de acceso restringido, servicios de mensajería encriptada como Telegram e incluso a la dark web (Canales, 2017), donde se debe acceder de manera deliberada y por tanto son radicalizados individuos que buscan de inicio el contacto con la organización y sus satélites activamente.

A pesar de que la respuesta a nuestra pregunta de investigación de si las capacidades españolas, como miembro de la comunidad internacional y ejemplo de lo existente en otros países del entorno, están preparadas para hacer frente al desafío ciberterrorista es positiva, otro de los puntos que queremos tratar en estas conclusiones es la mejora de las capacidades en cuanto a propuestas de futuro. En este sentido, la mejora de las capacidades actuales pasa por una detección temprana, por un entrenamiento continuo en escenarios probables, como ya se hace en el marco de la OTAN, pero ampliado a la coordinación de todos los sectores, incluido el privado.

Será clave la determinación temprana de la motivación de los ciberataques, es decir, si estamos ante una motivación puramente económica, hablaremos de ciberdelincuencia común y se pondrán en marcha las capacidades para este fin; si la finalidad es el ataque para la merma de las capacidades militares, económicas o sociales de un Estado por parte de otro Estado, estaremos en un caso de ciberguerra y si a esto le añadimos el ataque por parte de un grupo con una atribución de fines políticos, ideológicos o religiosos, sí podremos hablar de ciberterrorismo. Somos conscientes que, en papel, esta diferenciación es sencilla y que la complicación estriba en la atribución de responsabilidades en un mundo líquido, como en el que nos encontramos.

Y aquí, antes de acabar, hay que añadir una mejora que se refiere a la integración del conocimiento criminológico en cuanto a la oportunidad criminal en el ciberespacio y a la influencia del factor humano en la ciberseguridad. En el primer caso, se ha podido comprobar que las características intrínsecas (no existencia de tiempo y espacio) y extrínsecas (transnacionalidad, universalidad, neutralidad, apertura al cambio y en revolución permanente) (Miró, 2012 : 143-160) hacen de este espacio como preferible para actos de terrorismo tradicional amplificado, porque, de momento y como hemos reflejado aquí, un ataque ciberterrorista de calado en el que se produzca la pérdida de vidas humanas no parece ser factible, aunque haya habido intentos serios en los últimos años, como el intento de envenenamiento de una planta potabilizadora en Inglaterra por parte de Daesh alterando los parámetros de depuración a través de un ciberataque en 2018 (Zuloaga, 2018).

Y, por último, en cuanto a la coordinación deberíamos ver normal la colaboración y coordinación por parte de todas las capacidades nacionales e internacionales, incluso si aún no se ha determinado si es el ataque de un Estado, de un grupo terrorista, de un grupo ciberhackivista o de un cibercriminal (o grupo de ellos), incluidas las capacidades operativas militares. Todo ello debido a que la evolución de este fenómeno hace que cada vez sea más complejo determinar las relaciones entre unos y otros actores implicados.

Y sí podemos concluir con la validación de la hipótesis de partida en función de la red de capacidades expuestas aquí en el caso español, que puede ser extrapolable al ámbito internacional. Además de que todo lo observado en este estudio nos indica que la colaboración y coordinación será global o no lo será, porque los ciberataques terroristas del futuro y el aprovechamiento del ciberespacio por estos grupos ya es global.

5.Bibliografía

Bas, E. (1999). Prospectiva. Cómo usar el pensamiento sobre el futuro. Barcelona: Ariel Social

Canales, P. (2017). Las nuevas armas mediáticas del Daesh. Revista Española de Defensa (338), 46-51.

Cano Paños, M. A. (2019). La expansión, intensificación y seducción del terrorismo islamista a través de internet: análisis criminológico. Revista Científica General José María Córdova, 17(26), 271-287

Cano Paños, M. A & Castro Toledo, F. (2018). El camino hacia la (Ciber)Yihad. Revista Electrónica de Ciencia Penal y Criminología, 20

Center of Excellence Defence Against Terrorism. (2008). Responses to Cyber Terrorism. NATO science for peace and security series. Sub-series E: Human and societal dynamics. Ankara: IOS Press

Centro Criptológico Nacional (CCN-CERT) (2019). Misión y objetivos del CCN-CERT. https://www.ccn-cert.cni.es/sobre-nosotros/mision-y-objetivos.html, consultada el 3 de septiembre de 2019

Centro Criptológico Nacional (CCN-CERT) (2019). Ciberamenazas y tendencias. Madrid: Ministerio de Defensa

Centro Criptológico Nacional (CCN-CERT) (2018). Aproximación española a la ciberseguridad. Madrid: Ministerio de Defensa

Congreso de los Diputados (2018). Diario de Sesiones de las Cortes Generales XII Legislatura, núm. 105., Comparecencia de don Javier Candau Romero, Jefe del Departamento de Ciberseguridad del Centro Criptológico Nacional. Madrid. Recuperado el 31 de mayo de 2019, de http://www.congreso.es/public_oficiales/L12/CORT/DS/CM/DSCG-12-CM-105.PDF

Consejo de Seguridad Nacional. (2019). Estrategia Nacional de Ciberseguridad. BOE 30 de abril de 2019.

Cooperative Cyber Defense Center of Excellence (CCDCE) (2020). https://ccdcoe.org/

Denning, D. (1 de noviembre 2001). Is Cyber Terror next? U.S Social Science Research Council. Nueva York. Recuperado el 2 de junio de 2019 de https://poli.hevra.haifa.ac.il/~terror/homer/27.9.02/cyber%20terrorism.htm

Departamento de Seguridad Nacional (DSN) (2017). Estrategia de Seguridad Nacional 2017. Madrid: Presidencia del Gobierno. Recuperado el 19 de junio de 2019, de https://www.dsn.gob.es/sites/dsn/files/Estrategia_de_Seguridad_Nacional_ESN%20Final.pdf

Estado Mayor de la Defensa (EMAD) (2020). Mando conjunto de ciberdefensa. Recuperado de https://emad.defensa.gob.es/unidades/mccd/ el 10 de enero de 2020

Europa Press (22 de noviembre de 1997). ETA difunde propaganda en Internet para eludir el delito de apología del terrorismo, según la Guardia Civil. El Mundo. Recuperado el 10 de junio de 2019, de https://www.elmundo.es/navegante/97/noviembre/22/delitoseta.html

Escrivá, Á., & Lázaro, F. (28 de abril de 2014). 21 detenidos por usar las redes sociales para enaltecer el terrorismo y ofender a las víctimas. El Mundo. Recuperado el 11 de junio de 2019, de https://www.elmundo.es/espana/2014/04/28/535e47a2e2704ef91e8b4572.html

Guardia Civil (2019). Grupo de Delitos Telemáticos. Recuperado el 25 de septiembre de 2019 de https://www.gdt.guardiacivil.es/webgdt/la_unidad.php

Guardia Civil (13 de abril de 2016). La Guardia Civil detiene a 13 personas en una operación abierta contra el enaltecimiento del terrorismo en las redes sociales. Recuperado el 11 de junio de 2019, de http://www.guardiacivil.es/es/prensa/noticias/5713.html

Holt, T.; Bossler, D. & Seigfried-Spellar, K. (2015). Cybercrime and Digital forensics. An Introduction. New York: Routledge

Instituto Nacional de Ciberseguridad (INCIBE) (2019). Qué es INCIBE. Recuperado de https://www.incibe.es/que-es-incibe el 19 de enero de 2020

Jenkins, B. (1982). Statements about terrorism. (A. A. Science, Ed.) The Annals of the American Academy of Political and Social Science, 463, 12

Lesaca Esquiroz, J. (2017). Armas de seducción masiva (Primera ed.). Barcelona: Península.

López-Fonseca, O. y Pérez, F.J. (2019). La Audiencia Nacional investiga los movimientos de espías rusos en Cataluña. El País. Madrid. España. https://elpais.com/politica/2019/11/20/actualidad/1574276025_237776.html Consultado el 20 de enero de 2020.

Maras, M.H. (2017). Cybercriminology. London: Oxford university Press

Ministerio de Defensa (2014). Al-Ándalus 2.0: la ciber-yihad contra España. Granada: GESI (Universidad de Granada)

Miró, F. (2012). El cibercrimen. Fenomenología y Criminología de la delincuencia en el ciberespacio. Madrid: Marcial Pons.

Nieto Fernádez, I. (2018). La letalidad del ciberterrorismo. Revisa General de Marina. Ministerio de Defensa de España.

Ogun, M.N. (2015). Terrorist Use of Cyberspace and Cyber Terrorism: challenges and responses. Ámsterdam: IOS Press

Organización del Tratado del Atlántico Norte (OTAN) (2020). Ciberdefensa. Recuperado el 20 de enero de 2020 de https://www.nato.int/cps/en/natohq/topics_78170.htm

Pettinari, D. (1997), "Cyber Terrorism-Information Warfare in Every Hamlet," Police Futurist 5, n. 3: 7-8.

Rapoport, D. C. (2002). The Four Waves of Rebel Terror and September 11. Antropoethics, 8(1).

Torres Soriano, M. (2009). La dimension propagandistica del terrorismo yihadista global.

Unidad de Delincuencia Especializada y Violenta (UDEF) (2019). Quiénes somos. Recuperado el 25 de septiembre de 2019 de https://www.policia.es/org_central/judicial/udef/bit_quienes_somos.html

Zuloaga, J.M. (2018). El Estado Islámico intentó hackear una depuradora y envenenar el agua de miles de personas en Inglaterra. La Razón, Madrid, España, https://www.larazon.es/espana/el-estado-islamico-intento-hackear-una-depuradora-y-envenenar-el-agua-de-miles-de-personas-en-inglaterra-CH20148208/ consultado el 20 de enero de 2020.

Notas

1 El manuscrito forma parte de una estancia de investigación de Francisco José Girao González del programa español I +D+i en la Universidad a Distancia de Madrid (UDIMA).