Cuadernos de la Guardia Civil

Revista de Seguridad Pública

Núm. 54-2017

GOBIERNO DE ESPAÑA
MINISTERIO DEL INTERIOR
GUARDIA CIVIL
DIRECCIÓN GENERAL

CUADERNOS DE LA GUARDIA CIVIL

REVISTA DE SEGURIDAD PÚBLICA

3ª ÉPOCA

Centro de Análisis y Prospectiva de la Guardia Civil
Guzmán el Bueno, 110
28003 MADRID
Teléf. 91 514 29 56
E-mail: CAP-cuadernos@guardiacivil.org

AUTORA Y PROPIETARIA

Dirección General de la Guardia Civil
ISSN: 2341-3263
NIPO: 126-15-005-2

EDITA

Ministerio del Interior
Secretaría General Técnica
Dirección General de la Guardia Civil
Centro Universitario de la Guardia Civil

Página oficial de Cuadernos de la Guardia Civil
http://bit.ly/1Fdw213

Lista de los números en KOBLI
http://bibliotecasgc.bage.es/cgi-bin/koha/opac-shelves.pl?viewshelf=59&sortfield=

Catálogo general de publicaciones oficiales
http://publicacionesoficiales.boe.es/

A lo largo de los años, la Guardia Civil ha venido haciendo una gran labor divulgativa con la publicación de la Revista de Estudios Históricos, lo que ha contribuido a la comprensión de su carácter, su tiempo, sus actividades y funciones.

Desde 1989 este esfuerzo en difusión de cultura de seguridad ha desembocado en la elaboración de los "Cuadernos de la Guardia Civil".

Se trata de una publicación académico profesional, de contenidos originales y periodicidad semestral, con contenidos relevantes sobre seguridad nacional, seguridad pública, técnica policial, riesgos y amenazas, en todas sus dimensiones (histórica, jurídica, estratégica, táctica, etc.). Los géneros documentales admitidos son los artículos de investigación, los artículos profesionales, y la reseña de libros. Los destinatarios son expertos en seguridad, académicos y profesionales, tanto del sector público y privado, estudiantes, así como cualquier ciudadano interesado en la materia.

Cuadernos de la Guardia Civil está abierta a cualquier autor, a cuyos efectos se establecen dos periodos para la recepción de artículos: el 1 de mayo y el 1 de noviembre. El primer número de cada año se publica durante el mes de enero, y el segundo durante el mes de julio. Se pueden publicar adicionalmente números especiales o suplementos. Los artículos propuestos serán enviados respetando las normas de publicación que figuran al final del número. Las propuestas se pueden enviar en formato electrónico a: CAP-cuadernos@guardiacivil.org

La evaluación y selección de los artículos se realiza previa evaluación mediante un sistema por pares, en el que intervienen evaluadores externos a la editorial, y posterior aprobación por el Consejo Editorial. Los artículos pueden ser escritos en español, inglés o francés.

La Revista Cuadernos de la Guardia Civil se compromete a mantener altos estándares éticos, y especialmente el "Code of conduct and best practices guidelines for journal editors" del Committee on Publication Ethics (COPE).

Los contenidos de la Revista Cuadernos de la Guardia Civil se encuentran referenciados en los siguientes recursos de información: LATINDEX, DICE (Difusión y Calidad Editorial de las Revistas Españolas de Humanidades y Ciencias Sociales y Jurídicas) y DIALNET.

Especial referencia merece su inclusión en el sistema bibliotecario de la Administración General del Estado, a través de la Plataforma KOBLI:

http://bibliotecasgc.bage.es/cgi-bin/koha/opac-shelves.pl?viewshelf=59&sortfield=

Este servicio permite consultar y realizar búsquedas por cualquier criterio bibliográfico (autor, tema, palabras clave…), generar listas. Permite la descarga en formatos PDF, Mobi y Epub. Adicionalmente es posible la suscripción a un sistema de alerta, cada vez que se publique un nuevo número, solicitándolo a la cuenta : CAP-cuadernos@guardiacivil.org.

ÍNDICE

ARTÍCULOS

RESEÑA DE LIBROS

LA SEGURIDAD AEROPORTUARIA FRENTE AL TERRORISMO YIHADISTA: HORA DE REVALORIZAR LA PREVENCIÓN

JOSÉ ÁNGEL ASTILLERO FUENTES

TENIENTE CORONEL D.E.M. DE LA GUARDIA CIVIL

RESUMEN

En la deriva del yihadismo hacia una guerra total en suelo europeo los aeropuertos y la aviación civil siguen siendo, si cabe todavía más, un objetivo preeminente. Con estructuras terroristas difícilmente permeables a la investigación y dinámicas impredecibles, la prevención cobra un papel renovado en la respuesta antiterrorista. La amenaza *insider* o los ataques *inghimasi*, flamantes iconos del nuevo terrorismo, exigen soluciones integrales y audaces. Repensar la misma arquitectura de seguridad de nuestros aeropuertos, articular mecanismos de detección temprana del radicalismo o asumir la reacción policial a los ataques, sin el concurso de fuerzas especiales, son algunas de las líneas de acción sugeridas en este documento que identifica en el compromiso total de la sociedad la condición previa de su éxito.

Palabras clave: seguridad aeroportuaria, terrorismo yihadista, *insider*, *inghimasi*, prevención, respuesta policial.

ABSTRACT

Jihadism's drift toward a total war on European soil keeps seeing airports and civil aviation as an increasingly prominent target. Terrorist structures that are hardly permeable to investigation and unpredictable dynamics force prevention to play a renewed role within the counter-terrorism response. Insiders' threats (or inghimasi attacks), which are the brand-new icons of modern terrorism, require smart and integral solutions. Rethinking the very same security architecture of our airports, developing early warning systems to detect radicalism or assuming that police response to terrorist attacks is going to take place, without help from special operations teams, are just some of the courses of action suggested in this paper which identifies the civil society's full engagement as the precondition for success.

Keywords: airport security, jihadist terrorism, insider, inghimasi, prevention, police response.

1. INTRODUCCIÓN

Al abordar el estudio de la seguridad aeroportuaria frente a la amenaza yihadista la primera idea que asalta al analista es, paradójicamente, la sospecha de estar examinando un concepto que ha sido ya superado por la realidad. Efectivamente, desde hace mucho tiempo, la seguridad aeroportuaria ha sido fagocitada por el más amplio concepto de seguridad del transporte aéreo. Esta constatación, que por obvia puede antojarse *quasi* perogrullada, conviene no perderla de vista si se pretende llevar a

cabo un examen serio, preciso y contextual de la cuestión. Porque, *nolens volens*, cualquier brecha de seguridad que se produzca en un aeropuerto va a afectar de manera indefectible a la globalidad del transporte aéreo internacional.

El punto de partida de este estudio resulta preocupante. Según datos aportados por EUROPOL en su Informe sobre la Situación y Evolución del Terrorismo, durante el año 2015 fallecieron en territorio europeo 151 personas y 360 resultaron heridas como consecuencia de los 211 ataques terroristas (ejecutados, abortados y fallidos) registrados en seis Estados miembros de la Unión. Una Unión Europea en la que se detuvo, ese mismo año, a 1.077 individuos por presuntos delitos relacionados con el terrorismo; pero, sobre todo, más allá de la alarma que estas cifras generan, una Unión Europea en la que subyace el desasosiego, la inquietud y la incertidumbre a la hora de afrontar con garantías la amenaza terrorista que suponen los actores (lobos) solitarios.

2. INVESTIGACIÓN *VERSUS* PREVENCIÓN

Tales dificultades operativas para detectar y anular la actividad de estos elementos terroristas aislados –dificultades abiertamente reconocidas por EUROPOL en el citado informe– son consecuencia de la desconcertante (¿última?) deriva del yihadismo. Son ya varios los llamamientos realizados por el autodenominado Estado Islámico (en adelante DAESH) a sus militantes instándoles a atacar a Occidente con todos los medios a su alcance[1]. Esta apelación global, amplificada a través del impresionante aparato de propaganda desplegado por el DAESH, sin precedentes en la historia del terrorismo internacional, ha cristalizado en una "no-estructura" de su armazón terrorista, una atomización inconexa de sus piezas que intuitivamente se antoja más próxima a la anarquía que a cualquier otro tipo de patrón organizativo. Todo lo cual no ha sido fruto de la casualidad, más bien siguiendo al principio que sustenta la yihad individual: "la organización debilita"[2].

En este nebuloso y movedizo escenario la figura del *would-be terrorist* (terrorista potencial) trae de cabeza a los servicios de inteligencia y fuerzas policiales: ¿cómo detectar a tiempo a un individuo "no fichado" que ataca donde, cuando y como quiere?

En el terrorismo de corte clásico –por diferenciarlo terminológicamente del actual contexto yihadista– la propia esencia y dinámica terrorista constituía, o al menos daba oportunidades para ello, su talón de Aquiles. Se trataba de un modelo operativo que pivotaba en torno a una célula o comando, un grupo en definitiva cuya actividad se articulaba a través de interacciones internas y externas.

Así, para sus contactos entre miembros de la célula, éstos debían recurrir al empleo de teléfonos o internet o, en su defecto, evocando praxis ya trasnochadas pero en

1 Este tipo de llamamiento en realidad no es nada novedoso. En la obra "Llamada a la resistencia islámica global" aparecida en internet a finales de 2004, cuya autoría se atribuye a Mustafá Setmarian, terrorista con pasaporte español vinculado a las cúpulas de Al Qaeda y posteriormente del Estado Islámico, se postularon las bases de la denominada "yihad individual", exhortando a "golpear donde puedas, cuando puedas y como puedas". Pérez Ventura, Oscar. (2014). Mustafá Setmarian: el ideólogo de la yihad moderna. Instituto Español de Estudios Estratégicos. (Nótese, curiosamente, la similitud del llamamiento con el inicio del lema de los templarios: "Haz lo que puedas. Con lo que tengas. En donde estés. Pero siempre llévanos a la Gloria").

2 "Llamada a la resistencia islámica global", obra atribuida a Mustafá Setmarian.

su momento eficaces, buzones ocultos en el campo, correos humanos o citas personales. Cualquiera que fuese el elegido de estos métodos, la resultante era siempre la misma: se dejaban pistas, restos de una actividad de algún modo rastreable que eran, en definitiva, "investigables".

Además de una dinámica interna el grupo desarrollaba una actividad externa, aún más necesaria, si cabe, para alcanzar sus objetivos. La imagen del aquí acuñado terrorismo de corte clásico ha estado invariablemente ligada a vehículos bomba, ametrallamientos, secuestros y artefactos explosivos. En otras palabras, sus *modus operandi* dependían de manera intrínseca de la disponibilidad de armas, explosivos e infraestructura logística como pisos francos o *zulos*. Y esta dependencia obligaba a la célula bien a interactuar con otras estructuras de la organización terrorista –responsables del abastecimiento de armas y explosivos o la financiación para conseguir dichas infraestructuras–, bien a establecer contactos clandestinos con traficantes de armas –telefónicos, personales mediante intermediarios o en la *dark web*–. De nuevo, la misma resultante: indicios y rastros "investigables".

Sintetizando, la sinapsis interna y externa de los grupos terroristas constituía una fuente de oportunidades y posibilidades de investigación para los servicios antiterroristas. Pues bien, poco o nada de eso ocurre en la actual estrategia de los lobos solitarios (admitiendo que el recurso a esta anárquica figura merezca denominarse estrategia).

Efectivamente, la irrupción en escena de estos incontrolados e impredecibles actores solitarios ha cambiado las reglas del "juego" antiterrorista, introduciendo tres nuevos desafíos.

En primer lugar, el desafío ligado a su propia génesis. La sospecha es que, en no pocas ocasiones, la radicalización de estos individuos se produce al margen de los círculos próximos al yihadismo, es decir, fuera de los ámbitos que en mayor o menor medida son monitorizados por los servicios antiterroristas. Para que la simiente de la radicalización se deposite en estos sujetos no es necesario visitar webs terroristas o de apología de la yihad, ni tan siquiera acudir a reuniones y tertulias de fundamentalistas. En estos individuos podría bastar el mensaje de un imán radical al que ocasionalmente escucharon en la mezquita o, simplemente, los *inputs* de la propaganda yihadista que a diario bombardea a cualquier ciudadano a través de la normal información mediática. Esta simiente de radicalización, por tanto, no dejaría rastros investigables, y germinaría hasta dar sus frutos "oculta" en un recóndito lugar de la mente de estos sujetos adonde ningún micrófono, confidente o investigador pueden acceder.

En segundo lugar, la actuación del lobo solitario conlleva la dificultad certificada por su propia denominación: actúa aisladamente, en solitario, prescindiendo de contactos con otros terroristas. Lo que significa que tampoco aquí van a encontrarse indicios "investigables".

El tercer desafío deriva de los más recientes *modus operandi* escogidos por estos actores solitarios: el empleo de objetos de uso cotidiano como armas. Esta inquietante tendencia supone la sustitución de armas convencionales, cuya adquisición o tenencia son, *a priori*, siempre "investigables", por objetos como cuchillos o vehículos cuya adquisición o tenencia no son nunca, *per se*, "investigables". Una vez más, ausencia de pistas.

De todo cuanto ha sido expuesto podría deducirse a modo de corolario que la investigación, herramienta tremendamente eficaz frente al viejo terrorismo, encuentra complejas e inquietantes dificultades operativas ante la opacidad de los lobos solitarios del nuevo terrorismo. Lo cual abre el paso, como opción en el diseño de la respuesta antiterrorista, al fortalecimiento de la actividad preventiva.

3. MÁS Y RENOVADA PREVENCIÓN EN LOS AEROPUERTOS

Ante la comprometida situación de las herramientas investigativas los focos se centran, pues, sobre la prevención, esperando de ella soluciones que las fuentes vivas, las intervenciones telefónicas y los equipos de seguimiento parecen no poder aportar.

En ese nuevo papel emergente de la prevención, uno de los primeros debates planteados en el ámbito de la seguridad del transporte aéreo ha sido el de la necesidad de repensar la organización general de la seguridad aeroportuaria.

Este debate tiene su origen en el atentado contra el Aeropuerto de Bruselas (22.02.16) y las medidas adoptadas como consecuencia del mismo, en concreto el filtro de seguridad que las autoridades belgas decidieron implantar como paso previo para acceder a la terminal. Es decir, un filtro adicional en la zona pública situado antes del filtro que separa el lado tierra del lado aire.

Pues bien, un filtro semejante existía ya en el Aeropuerto Ataturk de Estambul cuando fue atacado por un comando yihadista el 28.06.16. Y lo que es más, antes de ese filtro previo dicho aeropuerto disponía de otro filtro para vehículos. Por ilustrarlo más gráficamente, un pasajero que pretenda embarcar en un avión en el Aeropuerto de Estambul debe someterse a tres controles de seguridad: un primer filtro selectivo de vehículos, seguidamente un filtro de seguridad para personas en el acceso a la terminal y por último el filtro para pasar al lado aire o zona restringida.

Los argumentos presentados a favor y en contra de esta arquitectura de seguridad en profundidad pueden condensarse a través de dos preguntas. La primera, acerca de sus efectos sobre la voluntad, la determinación de atentar de los terroristas. Evidentemente, y a la vista de los hechos, la respuesta es bastante obvia. Un mayor número de filtros de seguridad no es por ahora, ni en un futuro parece que lo vaya a ser, disuasión suficiente para los terroristas. La segunda pregunta versa, en cambio, sobre los resultados y las consecuencias de un ataque. Aquí resulta difícil dar una respuesta categórica, pero pueden esbozarse un par de ideas al respecto. De un lado, no deja de ser cierto que este tipo de dispositivos en profundidad aleja (interponiendo mayor distancia) la amenaza terrorista de las aeronaves y su pasaje, a la vez que permite adelantar la respuesta policial; en definitiva, se protege mejor el *core* del transporte aéreo, esto es, los aviones y sus pasajeros. De otro lado, como quiera que parezca plausible aceptar una mayor concentración humana en el lado aire de los aeropuertos, en cierto modo se reduce el potencial número de víctimas de un ataque.

En cualquier caso el debate sigue abierto y las dificultades estructurales y organizativas (y, dicho sea de paso, sus implicaciones económicas) que supone la implantación de tales dispositivos invitan a suponer que la cuestión no será resuelta en el corto o medio plazo.

4. REACCIÓN Y ADAPTACIÓN

La actividad preventiva que exige este nuevo escenario debe ser capaz de responder tempestivamente a la evolución de la amenaza. También en este aspecto el atentado del Aeropuerto de Estambul constituye un buen repositorio donde recabar ideas.

Dejando aparte cuestiones relacionadas con la *business continuity* (si bien no puede sino celebrarse la rápida recuperación de las operaciones, en tan solo unas horas, frente a las dos semanas del caso belga), apenas unos días después del ataque el gestor aeroportuario turco puso en marcha una serie de medidas, entre las cuales van a destacarse dos.

La primera, la protección de las terminales con barreamientos de hormigón. Resulta curioso, cuanto menos, que esta medida se adoptase pocos días antes del atentado perpetrado en Niza (14.07.16), en el que se empleó un camión para atropellar a la multitud congregada en el paseo marítimo de esa localidad durante la celebración de la fiesta nacional francesa[3]. Al margen de esta anticipación proactiva en el diseño preventivo y sin entrar a barajar posibles hipótesis sobre la información (¿privilegiada?) disponible que motivó la adopción de tal medida –más allá del ánimo de impedir el alunizaje de vehículos bomba en la terminal–, lo cierto es que una nueva vulnerabilidad de las instalaciones aeroportuarias ha sido puesta de manifiesto. Y una nueva inquietud también: ¿cuántos aeropuertos europeos están preparados para impedir atentados como el de Niza o Berlín?

La segunda de las medidas dispuestas por las autoridades turcas que merece mención es el incremento de la presencia policial robusta en las instalaciones aeroportuarias, entendiendo por robustez la articulación de servicios en patrullas, la protección de la fuerza mediante chalecos antiproyectiles y la dotación de armas largas. Y esto, que podría pasar inadvertido por la lógica simplista que anima la medida (a más amenaza más prevención) no es una cuestión baladí, porque denota una clara voluntad de reaccionar adaptando “cualitativamente” la respuesta a unos terroristas que, no está de más recordarlo, atacan indiscriminadamente masas de ciudadanos abriendo fuego con fusiles de asalto y lanzando granadas de mano para finalmente suicidarse con cinturones explosivos. Lo cual no es más que la réplica de los ataques *inghimasi* que, en el conflicto de Siria e Iraq, protagonizan combatientes paramilitares del DAESH al penetrar sin idea de retorno las líneas enemigas, esto es, para “inmolarse”.

5. INTROSPECCIÓN AEROPORTUARIA

Por si de los ataques a los aeropuertos de Bruselas y Estambul no se derivasen bastantes nuevos desafíos a la seguridad del transporte aéreo, los últimos atentados perpetrados contras aeronaves han añadido al asunto una ulterior vuelta de tuerca con la introducción de la denominada amenaza *insider*.

El 31.10.15 un avión de bandera rusa de la compañía METROJET, en vuelo entre Sharm el Sheick y San Petersburgo, se estrelló en el desierto del Sinaí como consecuencia de la explosión de un artefacto, falleciendo las 224 personas que iban a bordo.

3 *Modus operandi* posteriormente reproducido en el atentado terrorista perpetrado en Berlín el 19.12.16, cuando un camión embistió a decenas de personas en un mercadillo de Navidad del centro de la capital alemana, dejando 12 muertos y medio centenar de heridos.

El 02.02.16 durante el vuelo de un avión de bandera griega operado por HERMES AIRLINES estalla un artefacto explosivo, obligando a la aeronave a realizar un aterrizaje de emergencia en el aeropuerto de Mogadiscio, de donde había despegado minutos antes; afortunadamente, solo falleció el terrorista.

En el primero de los atentados, según las informaciones disponibles, el artefacto explosivo estaba oculto en una lata de refresco. En el segundo, camuflado en un ordenador portátil. La pregunta, en ambos casos, es cómo consiguieron los terroristas pasar los filtros de seguridad con los artefactos explosivos. La respuesta, muy sencilla: los terroristas no pasaron los filtros de seguridad con los artefactos. En el primer caso, alguien, con toda probabilidad un empleado aeroportuario, colocó el artefacto en la bodega *bulk* de la aeronave. En el segundo, tal y como registraron las cámaras del CCTV de seguridad del aeropuerto de Mogadiscio, un operario entregó el ordenador al terrorista una vez superado el filtro de seguridad, ya en el lado aire.

Aunque podría esgrimirse que el nivel de seguridad AVSEC de los aeropuertos de origen de los aviones siniestrados no representa un estándar válido al que pueda referenciarse la seguridad de los aeropuertos europeos, la amenaza *insider* no solo está presente en aeropuertos de regiones con una historia de pobreza, radicalismo y conflicto[4].

En cualquier caso no cabe duda que, por su gravedad, la amenaza *insider* no puede ser soslayada[5]. Y, una vez admitida, deben aceptarse todas sus consecuencias: los mecanismos de *vetting* que la normativa AVSEC contempla (SA-20 del Programa Nacional de Seguridad para la Aviación Civil) podrían resultar insuficientes para detectar y neutralizar la actividad *insider* en nuestros aeropuertos.

La radicalización de un individuo, como se ha visto, puede discurrir por cauces virtualmente indetectables a la acción de los servicios antiterroristas. Lo cual supone un *bypass* de las medidas articuladas en la SA-20, posibilitando hipotéticos escenarios en los que un sujeto debidamente autorizado por la normativa AVSEC se radicalice o incluso una vez radicalizado obtenga la preceptiva autorización.

La contextualización de la amenaza *insider* que aporta el perfil del autor de la masacre de Niza hace que estas situaciones pasen de ser consideradas “no descartables” a configurarse como “razonablemente probables”. Mohamed Lahouaiej-Bouhlel no solía acudir a la mezquita, no respetaba el ayuno durante el Ramadán y comía carne de cerdo con regularidad. Descrito por su entorno más cercano como un tipo solitario, este individuo consumía drogas y alcohol, era asiduo a locales nocturnos de baile latino y su vida personal estaba salpicada de episodios de agresividad social y violencia doméstica. Sin duda, su comportamiento se situaba en las antípodas del ideario fundamentalista y lo colocaba, consecuente pero erróneamente, fuera de la atención policial.

En la más que nunca guerra asimétrica que constituye la lucha contra el yihadismo suele caerse, inconscientemente, en la ingenuidad de aceptar como válido el

4 En un artículo titulado “Why the insider threat to airport security isn’t just Egypt’s problem”, Owen Matthews, colaborador habitual de Newsweek, sostiene esta tesis, presentando varios casos de incidentes insider en los aeropuertos de Newcastle (Reino Unido) y Wichita (USA). http://www.newsweek.com/2016/06/03/egyptair-metrojet-flight-9268-airport-security-462784.html

5 En 2015 el *Department of Homeland Security*, la TSA *(Transportation Security Administration)* y el FBI de los USA declararon la amenaza insider una prioridad. *White paper: The core of insider threat mitigation is identity & credential management*. www.quantumsecure.com. 2016.

arquetipo yihadista del imaginario colectivo: un tipo que no renuncia ni a los signos externos ni a las obligaciones religiosas que identifican su exacerbada y manipulada fe; si se prefiere, simplificando el asunto, alguien cuya presencia y modo de actuar preanuncian públicamente su militancia extrema.

Al igual que ETA, por citar un ejemplo a todos próximo, instruía a sus liberados para pasar desapercibidos en la sociedad, el DAESH aconseja a sus activistas que escondan su fe en Occidente[6]. Con toda probabilidad, en el caso del terrorista de Niza su perfil no era fruto de una acción consciente y buscada, pero la lección aprendida debe ser la misma. Deliberadamente o no, el perfil del yihadista se va a presentar, cada vez más, fuera de los patrones y clichés comúnmente esperados.

La SA-20, por tanto, es necesaria pero no suficiente. Además de su correcta aplicación[7] se requieren medidas adicionales que habiliten una más estrecha monitorización del personal laboral aeroportuario. Programas como CoPPRa (*Community Policing Prevention Radicalism & Terrorism*), puesto en marcha por AIRPOL, apostando por una directa implicación del mismo colectivo laboral aeroportuario como responsable en última instancia de su propia seguridad, permitirán recuperar y fortalecer la interacción de las fuerzas de seguridad con el ciudadano para, en definitiva, aportar una mayor profundidad en la detección temprana de elementos radicales[8].

Y no solo eso. Además de un mayor alcance en el control, se requiere una ampliación de su extensión. Mantener una frontera entre el lado aire y el lado tierra para delimitar el coto del *vetting* supone, incomprensiblemente, debilitar la seguridad de una zona pública que, además de desarrollar su actividad cotidiana en constante simbiosis con la zona restringida, ha sido el escenario de la mayoría de los últimos atentados perpetrados contra instalaciones aeroportuarias.

Junto a esta mayor capacidad de *vetting,* se antoja que deben ser exploradas soluciones integrales de mitigación de la amenaza *insider*[9] y han de articularse otras

6 Son diversos los mensajes lanzados en este sentido, todos ellos amparados por la doctrina de la *taqiylla* que, basándose en diversos preceptos del Corán, permite la mentira y el engaño a los infieles para favorecer el islam, su conquista del mundo o la defensa individual de un musulmán. Sobre el asunto, véase, entre otros: Riga, Peter J. *ISIS, fundamentalism and Islam: insights into America's mortal enemies*. Authorhouse, 2015; Widlanski, Michael. *Battle for our minds: Western elites and the terror threat*. Threshold Ed., 2012.

7 En 2015 una auditoría realizada por el *Department of Homeland Security* de USA sobre los mecanismos de control de acreditaciones aeroportuarias de la TSA puso de relieve que 73 empleados aeroportuarios y de compañías aéreas habían conseguido sus acreditaciones a pesar de poseer antecedentes policiales relacionados con el terrorismo. Según el informe de la auditoría, estos errores habrían tenido como causa la imposibilidad de la TSA para acceder a toda la información antiterrorista que a nivel interagencias se dispone en USA. Abdullah, Halimah. (2015). *TSA Fails to ID 73 Airport Employees With Links to Terrorism.* http://www.nbcnews.com/news/us-news/tsa-fails-identify-73-employees-terror-watch-lists-n371601

8 Este programa está siendo implementado por las Unidades de Seguridad Aeroportuaria de la Guardia Civil de Madrid (Barajas) y Barcelona (El Prat).

9 Como la adoptada en el Aeropuerto Internacional de Richmond-Virginia. Este tipo de solución vincula, en un único sistema, la gestión de identidades y credenciales junto a las infraestructuras de seguridad aeroportuaria y herramientas de análisis predictivo, permitiendo, mediante la definición de una serie de indicadores de compromiso, detectar y dar respuesta a conductas sospechosas. Gelles, G. Gelles. *Insider Threat Mitigation. Considerations for Building an Industry Leading Insider Threat Program*. Deloitte Consulting. http://aci-na.org/sites/default/files/aci_deloitte_presentation.pdf. http://www.airportimprovement.com/article/richmond-intl-pitches-paper-saves-time-new-identitymanagement-software

medidas adicionales al ámbito AVSEC, como por ejemplo inspecciones aleatorias de personal laboral o empleo de perros detectores de explosivos, tanto en la zona pública como en la restringida, cobrando, en este último caso, una crucial importancia su empleo en los reconocimientos preventivos de aeronaves.

Reconocimientos preventivos de aeronaves que, por cierto, han estado en el ojo del huracán tras el siniestro aéreo que el 19.05.2016 tuvo lugar en aguas del Mediterráneo, cuando un Airbus A-320 de la compañía EGYPTAIR, el ya fatídico vuelo MS804, se estrelló con 66 personas a bordo por causas aún no del todo esclarecidas.

El avión, con destino a El Cairo, partió del aeropuerto parisino Charles de Gaulle y cuando se encontraba a 280 kilómetros de la costa egipcia desapareció del radar. Poco antes, el sistema ACARS de la aeronave (sistema de información y dirección de comunicación) había emitido un mensaje automático alertando de la presencia de fuego en el interior de los baños del avión.

Los datos disponibles no descartaron en su día que el siniestro hubiera sido provocado por la explosión de un artefacto explosivo, pero tampoco lo confirmaron. Los ulteriores desarrollos de este dramático episodio quedaron marcados por la especulación cuando, en septiembre del mismo año, *Le Figaro* publicó que investigadores de la Gendarmería del Transporte Aéreo habrían encontrado posibles trazas de explosivo TNT en los restos del avión. Finalmente, el 15.12.2016 la especulación adquirió visos de realidad tras el anuncio oficial del Comité de Investigación de Accidentes Aéreos de Egipto: se confirmaba la presencia de residuos explosivos en los restos humanos de las víctimas.

Aparte del DAESH, el único beneficiado por la consolidación de la hipótesis de un atentado es el consorcio AIRBUS. Orillando estériles reflexiones sobre el interés del gigante europeo de la industria aeronáutica en descargar de sus espaldas cualquier responsabilidad del siniestro, los perjudicados son, una vez más, los aeropuertos.

El mismo día del incidente, antes de aterrizar en Paris, el MS804 había hecho escala en El Cairo (Egipto), Asmara (Eritrea) y Túnez (Túnez). Sin ningún tipo de datos disponibles, solo cabe conjeturar que la introducción de un artefacto explosivo en la aeronave podría haber tenido lugar en cualquiera de los cuatro aeropuertos. En los casos de Egipto, Eritrea y Túnez, el grado de actividad y presencia yihadista de esos países, de una parte, y los estándares de seguridad de sus aeropuertos, probablemente no ejemplares, de otra parte, explicarían lo (presuntamente) sucedido. En el caso de Francia, para más inri en el emblemático aeropuerto de Roissy-Charles de Gaulle, las explicaciones no terminan de convencer a nadie.

Que Francia está en el punto de mira del yihadismo resulta obvio, como lo es la excepcional y firme respuesta que las autoridades francesas están dando para luchar contra la barbarie que azota al vecino país. En el marco de esa respuesta, durante el año 2015 se revocó, por presentar signos de radicalización, la acreditación a 70 empleados aeroportuarios franceses (de un colectivo total de 85.000). Mas, a la vista de lo sucedido, esta medida no habría bastado. Desde luego ayuda a controlar el riesgo *insider*; *s*in embargo no lo neutraliza. La sospecha está ahí: el (presunto) artefacto bien pudo haber ser introducido durante la escala de la aeronave en Paris. También en cualquiera de las otras escalas, por supuesto. Pero no puede ni, sobre todo, debe descartarse la hipótesis más peligrosa: que el escenario de la acción fuese el aeropuerto parisino.

Por tanto, cabe hacer más, y en tal sentido lo pertinente sería complementar medidas como la anteriormente expuesta, la revocación de acreditaciones laborales aeroportuarias, con otras de distinta naturaleza enfocadas no tanto al control propiamente dicho de los *insiders* sino al de sus acciones. Como ha sido preanunciado, se está aludiendo a los reconocimientos preventivos de aeronaves, llevados a cabo entre la finalización de la limpieza y el inicio del embarque de pasajeros, para la búsqueda y localización de posibles artefactos explosivos.

Al margen de la preceptiva inspección atribuida a las tripulaciones que se desarrolla antes del inicio del embarque de pasajeros, las fuerzas policiales responsables de la seguridad aeroportuaria deben reconocer a fondo la aeronave. Especialmente en vuelos de compañías de bandera de Estados señalados por el DAESH (piénsese en Turquía o USA), y vuelos con destino o procedencia de esos Estados o con escalas en territorios donde el yihadismo cuenta con más implantación y apoyos. Para compensar el escaso tiempo disponible y maximizar la eficiencia de su acción, el equipo de inspección debe saber identificar los posibles lugares de ocultación de artefactos (por ejemplo en los lavabos o bajo los asientos) y recabar apoyos de unidades caninas adiestradas para la detección de explosivos. Parece plausible suponer que un reconocimiento de este tipo, de haberse llevado a cabo correctamente, habría eximido al aeropuerto Charles de Gaulle de muchas sospechas en el siniestro del MS804.

Con todo, el análisis de este trágico episodio no puede concluirse sin admitir que la presencia de residuos explosivos en los restos del avión no confirma inequívocamente la existencia de un artefacto explosivo. Durante las operaciones de rescate los restos de la aeronave se fueron disponiendo, a medida que se extraían del mar, sobre la cubierta de un buque de la marina de guerra egipcia[10]. La posibilidad de contaminación de los restos del avión y los cadáveres por los residuos explosivos que, con muy alta probabilidad, existen en la cubierta de una nave de guerra, abre un interrogante en el mismo instante de formular cualquier hipótesis.

Y el hecho de que hasta la fecha el DAESH no haya reivindicado el presunto atentado torna aún más turbio el asunto.

6. EL NUEVO ROL DEL AGENTE DE SEGURIDAD AEOPORTUARIA

El 20 de abril de 1999 dos estudiantes desequilibrados tirotearon a muerte a 15 compañeros y profesores e hirieron a otros 24 en la Escuela Secundaria de Columbine, Colorado. Sin ser, ni mucho menos, la más trágica de las masacres en centros educativos de los Estados Unidos, este incidente supuso un punto de inflexión en la respuesta policial a tan trágico tipo de ataques.

Efectivamente, tras una posterior revisión de lo sucedido, la actuación policial quedó en entredicho, al constatarse que las patrullas llegadas al lugar de los hechos se limitaron a acordonar la zona y se tardó demasiado en entrar en el edificio. El juicio crítico terminó por superar la doctrina hasta entonces indiscutida de cercar a los atacantes y aguardar hasta la llegada de unidades especiales (S.W.A.T.) y, en su lugar, constreñidos por una casuística marcada por el escaso margen de tiempo

10 Baum, Philip. (2016). *Special Report – MS804: explosive residue on victims confirmed. Aviation Security International – The Global Journal of Airport & Airline Security*.

disponible[11], los departamentos de policía norteamericanos empezaron a instruir a sus agentes para actuar apenas se llegara al lugar del incidente, sin esperar refuerzos.

A este otro lado del Atlántico masacres como las del Liceo Gutenberg de Erfurt (2002) en Alemania, el Instituto "Jokela" de Tuusula (2007) y el Instituto Profesional de Kauhajoki (2008), ambos en Finlandia, y la Escuela Secundaria "Albertville" de Winnenden (2009), nuevamente en Alemania, irían catalizando las mismas transformaciones en la respuesta policial a este tipo de ataques en masa.

El breve *excursus* realizado en la trágica historia de los *school shootings* pone de relieve un paralelismo irrefutable con la respuesta al nuevo paradigma terrorista. Desde el inicio de un ataque yihadista hasta la intervención policial median escasos minutos y los protagonistas de esa primera respuesta no serán fuerzas especiales de intervención, sino agentes o patrullas territoriales, en el caso de los aeropuertos en servicio de custodia de sus instalaciones o de seguridad ciudadana.

Por tanto, el desafío de los agentes de seguridad aeroportuaria no estriba únicamente en asumir las responsabilidades asociadas al renovado –según ha sido descrito en este documento– papel de la prevención, sino también en arrogarse la carga de constituir la primera (y muy probablemente única) línea de defensa y reacción. Así las cosas, no será, en muchas ocasiones, el servicio de inteligencia quien alerte de la presencia del terrorista, ni un equipo especial de intervención quien le haga frente.

La reacción en estos escenarios, a menudo solapada con la detección –típicamente anunciada al grito de "*Allah Akbar*" y ráfagas de AK-47– plantea nuevas exigencias formativas en el personal que presta servicios de seguridad aeroportuaria. Sin duda, las capacidades operativas básicas de estos agentes permiten afrontar con garantía y solvencia la gran mayoría de escenarios policiales; sin embargo, tales conocimientos y aptitudes deben ser re-evaluados ante la extrema exigencia de un ataque terrorista perpetrado con el empleo combinado de armas automáticas y explosivos.

Sin ánimo exhaustivo, estas acciones yihadistas se caracterizan por el efecto sorpresa –desencadenamiento súbito y simultáneo, en ocasiones coordinadamente en varios focos–, un desarrollo muy dinámico –con movimiento continuo y dispersión de sus autores en busca del caos y la maximización de los efectos del atentado– y una ausencia de estrategia de huida –el ataque se prolonga en el tiempo hasta que los autores son abatidos o se "inmolan"–.

A todo ello hay que sumar la singularidad del teatro de operaciones, con puntos de alta concentración de pasajeros (piénsese en los filtros de acceso a la zona restringida o en los mostradores de facturación), presencia de pasajeros con movilidad reducida y menores (frecuentemente en grupo), y desconocimiento generalizado de rutas de escape.

11 De un estudio del *Advanced Law Enforcement Rapid Response Training Center* (ALERRT) de la Universidad del Estado de Texas, llevado a cabo sobre 84 casos de tiroteos masivos ocurridos en USA entre 2000 y 2010, se desprende que el tiempo medio de respuesta policial en este tipo de ataques ronda los tres minutos. Sin embargo–añade el mismo estudio– la mitad de los incidentes ya han concluido cuando la policía se persona en el lugar de los hechos. Goode, Erica. (2013). *In Shift, Police Advise Taking an Active Role to Counter Mass Attacks. The New York Times*. http://www.nytimes.com/2013/04/07/us/in-a-shift-police-advise-taking-an-active-role-to-counter-mass-attacks.html

Con tales condicionantes, y contando exclusivamente con el personal y medios presentes en el momento del ataque, el dispositivo de seguridad aeroportuaria ha de ser capaz de combinar la neutralización de los terroristas con la protección y evacuación de civiles. Lo cual supone, ya se ha señalado, un plus formativo del personal, esencialmente orientado al desarrollo de tácticas operativas *ad hoc* capaces de conjugar la evacuación de pasajeros y personal laboral con la contención, mitigación y neutralización del ataque[12]. El perfecto conocimiento del entorno para poder activar distintas vías de evacuación o zonas de resguardo, el empleo de armamento y medidas de autoprotección adecuadas (estudiando, por ejemplo, la viabilidad del uso de escudos balísticos), la coordinación interagencias y la articulación de programas que impliquen activamente al ciudadano deberían sustentar el contenido de esta formación y adiestramiento[13].

7. A MODO DE CONCLUSIÓN: VOLUNTAD DE VENCER

Desde la Doctrina militar del año 1924, inspirada en la escuela militar francesa tras su experiencia en la Primera Guerra Mundial, hasta la actual Doctrina de 1976, derivada de la OTAN, los tres principios fundamentales de la guerra han variado sustancialmente con el paso del tiempo. Y sin embargo, uno de ellos ha permanecido siempre inmutable en la terna: la voluntad de vencer.

A medio plazo el colapso del DAESH parece inevitable. Todos los escenarios que se prospectan para el día después tienen un común denominador: el éxodo descontrolado de ex-combatientes. No resulta aventurado imaginar que gran parte de ellos, en una huída hacia adelante, cruzarán clandestinamente las fronteras europeas y acabarán instalándose entre el enemigo, Occidente, cobijados por radicales o familiares, cuando no bajo falsa identidad. Afrontar la amenaza de estas hordas de terroristas duramente adiestrados, curtidos en el combate y con un siniestro historial de atrocidades y barbaries con prisioneros y población civil, podría exigir de las sociedades europeas un grado de compromiso, resolución y firmeza solo parangonable al exhibido en las dos grandes guerras que asolaron el viejo continente durante el siglo pasado. Ofrecer "*sangre, esfuerzo, sudor y lágrimas*", como en 1940 hiciera al pueblo británico Sir Winston Churchill, no sería del todo descabellado.

A esta metástasis del DAESH en territorio europeo seguirán recrudecidos sus últimos estertores –ese es el temor celado de muchos analistas– y se pondrá a prueba

12 En este sentido, en la Guardia Civil se está estudiando la viabilidad del denominado Proyecto PRAT (Patrones de Reacción ante Ataques Terroristas), cuyas siglas hacen referencia al Aeropuerto del Prat de Barcelona, eventual escenario de esta iniciativa pionera.

13 Además de los 105.00 agentes de policía formados desde la creación del ALERRT en 2002 (en 2013 el FBI consideró el currículum formativo del ALERRT como estándar nacional y lo incorporó a sus programas de enseñanza), por este centro de excelencia de la Universidad del Estado de Texas han pasado 86.500 civiles, en el marco del programa *Civilian Response to Active Shooter Events* (CRASE). En palabras del director del ALERTT, Dr. J. Pete Blair, "en ausencia de presencia policial, la respuesta de las víctimas supone la diferencia entre la vida y la muerte". Así, en 16 de los 84 casos del estudio anteriormente citado, los civiles fueron capaces de neutralizar a sus agresores; en otros episodios su respuesta retardó y dificultó notablemente la acción del atacante, facilitando la posterior intervención de la policía. Diversos mensajes institucionales de Departamentos de Policía y Universidades de los USA, hasta del mismo *Homeland Security*, recomiendan a los civiles enfrentarse a sus atacantes si las opciones de escapar o esconderse no están disponibles. Goode, Erica. (2013).*op.cit.*

la fortaleza moral de los europeos, la preparación de sus capacidades antiterroristas y la resiliencia de sus infraestructuras, entre las cuales –no quepa la menor duda– los aeropuertos seguirán siendo un objetivo recurrente.

Porque, si los terroristas atacan el estadio Saint Denis de Paris, los aficionados al fútbol podrían dejar de ver partidos en directo y, en su lugar, seguirlos desde la televisión de sus hogares. Si atentan contra la sala Bataclán, los amantes de la música podrían dejar de ir a conciertos y, alternativamente, comprar discos. Incluso si se lanzan ataques contra el metro de Bruselas, autobuses en Londres o trenes en Madrid los ciudadanos podrían recurrir, en mayor o menor medida, a desplazarse con sus vehículos privados. Pero si los yihadistas siguen atacando aeropuertos o derribando aeronaves… ¿podríamos dejar de viajar?

En el mentado escenario del día después, tras el fallido califato, la coexistencia de actores solitarios "no fichados" con los para entonces recién llegados *former fighters* obligará a las fuerzas de seguridad de una parte, y según cuanto expuesto en este documento, a intensificar su actividad preventiva para detectar a los primeros y, de otra, para neutralizar a los últimos, a emplear todas y cada una de sus capacidades de investigación, tanto más cuando la tendencia de los ex-combatientes a asociarse en células será bastante probable.

Las medidas que hayan de adoptarse (las aquí propuestas y otras muchas que por brevedad expositiva quedan en el tintero), para la mejora del control y el desarrollo de instrumentos que refuercen la seguridad del transporte aéreo, deben articularse, obviamente, en un marco de exquisito respeto al conjunto de derechos y libertades que cimientan el modelo social europeo, en particular la protección de datos de carácter personal. No obstante, tampoco debe renunciarse, *a priori*, a eventuales cambios normativos que supediten el fin a los medios. Lo cual, anticipando voces críticas, no sería una cesión de libertad y privacidad en favor de la seguridad, sino en aras de la protección del más importante de los derechos, sin el cual todos los demás carecen de sentido: el derecho a la vida.

Y tampoco, en modo alguno, constituiría una abjuración de los principios y valores que vertebran el ideal europeo. Más bien, el compromiso solidario, responsable y consciente de una sociedad que afronta, con coraje y determinación, esta guerra declarada unilateralmente que es la yihad.

Si la guerra, como afirmara Clausewitz, no es más que un choque de voluntades[14], tal compromiso no vendría más que a reafirmar nuestra voluntad de vencer.

BIBLIOGRAFÍA

Abdullah, Halimah. (2015). TSA Fails to ID 73 Airport Employees With Links to Terrorism. http://www.nbcnews.com/news/us-news/tsa-fails-identify-73-employees-terror-watch-lists-n371601

Baum, Philip. (2016). Special Report – MS804: explosive residue on victims confirmed. Aviation Security International – The Global Journal of Airport & Airline Security.

Garrido Roca, Pedro. Seguridad aeroportuaria: respuesta de la Guardia Civil. Ponencia del Curso Avanzado de Seguridad Aeroportuaria – AENA. Barajas, 25.10.16.

14 Clausewitz, Carlo Von. (1832). De la Guerra. Ed. La Esfera, 2014.

Gelles, G. Gelles. Insider Threat Mitigation. Considerations for Building an Industry Leading Insider Threat Program. Deloitte Consulting. http://aci-na.org/sites/default/files/aci_deloitte_presentation.pdf

Goode, Erica. (2013). In Shift, Police Advise Taking an Active Role to Counter Mass Attacks. The New York Times. http://www.nytimes.com/2013/04/07/us/in-a-shift-police-advise-taking-an-active-role-to-counter-mass-attacks.html

Matthews, Owen. (2016). Why the insider threat to airport security isn't just Egypt's problem. http://www.newsweek.com/2016/06/03/egyptair-metrojet-flight-9268-airport-security-462784.html

Pérez Ventura, Oscar. Mustafá Setmarian: el ideólogo de la yihad moderna. Instituto Español de Estudios Estratégicos, 05/2014.

Riga, Peter J. (2015). ISIS, fundamentalism and Islam: insights into America's mortal enemies. Authorhouse.

Widlanski, Michael (2012). Battle for our minds: Western elites and the terror threat. Threshold Ed.

DARDO AVSEC 01/2015, 01/2016, 02/2016, 03/2016, 05/2016. Servicio de Costas y Fronteras, Dirección General de la Guardia Civil.

EUROPOL. (2016). Informe sobre la Situación y Evolución del Terrorismo.

White paper: The core of insider threat mitigation is identity & credential management. www.quantumsecure.com. 2016

http://www.secureamericanow.org/inghimasi_isis_s_deadly_tactial_approach

http://www.nbcnews.com/news/us-news/tsa-fails-identify-73-employees-terror-watch-lists-n371601

http://www.airportimprovement.com/article/richmond-intl-pitches-paper-saves-time-new-identitymanagement-software

Fecha de recepción: 03/11/2016. Fecha de aceptación: 20/12/2016

ENTREVISTA A PERSONAS VULNERABLES (MENORES) EN DELITOS CONTRA LA LIBERTAD SEXUAL

Mª JOSÉ GARRIDO ANTÓN Y JOSÉ LUIS GONZÁLEZ-ÁLVAREZ

SACD – UTPJ. SECRETARÍA DE ESTADO DE SEGURIDAD. GABINETE DE COORDINACIÓN Y ESTUDIOS

Los monstruos no tienen por qué ser engendros, ni fieras enloquecidas, quizá tampoco respondan al perfil de personas deshumanizadas y peligrosamente aversivas, los monstruos a veces resultan ser las personas que nos deberían proteger de ellos…

RESUMEN

El equipo central de psicólogos de Policía Judicial de la SACD juega un papel esencial a la hora de recoger el testimonio de personas vulnerables en delitos contra la libertad sexual. La entrevista semiestructurada a menores se ha convertido en la técnica por excelencia a la hora de investigar este tipo de delitos caracterizados por el abuso del poder. A través de ésta se intenta poner al descubierto todas las circunstancias y detalles sobre los hechos denunciados. La intención principal de estos agentes es, sin duda, la protección del menor y de víctimas especialmente vulnerables, la salvaguarda de la posible victimización secundaria y el esclarecimiento de los hechos con todas las garantías procesales.

Palabras Clave: Abuso sexual infantil, entrevista semiestructuradada, investigación policial, niños.

ABSTRACT

The Judicial Police's core team of psychologists (SACD) plays an essential role in collecting the testimony of vulnerable people in sexual abuse crimes. Semistructured interviews have become the quintessential technique in the investigation of such crimes, which are marked by abuse of power. Through this technique, the team tries to uncover all the circumstances and details of the allegations. Undoubtedly, the main intention of these agents is the protection of minors and vulnerable victims, safeguarding the possible secondary victimization and the clarification of the facts with all procedural safeguards.

Key words: Sexual abuse, semistructured interview, police investigation, children.

1. INTRODUCCIÓN

Casos de abusos y agresiones sexuales en personas vulnerables, siendo el porcentaje más voluminoso sobre menores, son ejemplo de las novedades con las que los componentes de la SACD[1] se encuentran semanalmente en la bandeja de entrada

1 Sección de Análisis del Comportamiento Delictivo de la Guardia Civil, primera unidad policial en España dedicada al análisis de la conducta de personas afectadas por delitos, tanto sospechosos como de víctimas y testigos, cuyo cometido es aplicar los conocimientos de la Psicología a la investigación policial (psicología criminalista), realizar determinados estudios estratégicos del comportamiento delictual y prestar los apoyos operativos pertinentes a las Unidades Orgánicas de la Policía Judicial.

de su correo corporativo. A raíz de estas comunicaciones automáticamente surgen los interrogantes sobre la credibilidad de los testimonios. La función como Policía Judicial de estos efectivos es tomar la declaración de los menores sin ningún tipo de interpretación a priori, ni inducción o sesgo que pueda influenciar el relato de los niños.

En primer lugar conviene indicar a quién se denomina "persona vulnerable". En este sentido el término *vulnerable* es definido por el Diccionario de la Lengua Española (DEL) como '*aquella persona que puede ser herida o recibir lesión física o moralmente*'. La Federación Internacional de Sociedades de la Cruz Roja (2010) lo define como la capacidad disminuida de una persona o un grupo de personas para anticiparse, hacer frente y resistir a los efectos de un peligro natural o causado por la actividad humana y para recuperarse de los mismos. González, Muñoz, Sotoca y Manzanero (2013) consideran vulnerables a las personas que tienen un mayor riesgo de sufrir una victimización secundaria[2] o re-victimización provocada por el sistema judicial, con una escasa capacidad para defender sus derechos sin ayudas e, incluso, con el riesgo de ser excluidas por el sistema. Se considera "personas vulnerables" a diversos colectivos, como son las personas con discapacidad (psíquica, física o sensorial), personas que sufren de un trastorno mental, o los menores de edad. Este artículo se va a centrar en estos últimos.

Conviene indicar que la propia Constitución Española de 1978 hace mención a la obligación de los Poderes Públicos de asegurar la protección social, económica y jurídica de la familia y, dentro de esta, con carácter singular, la de los menores, vinculándolo con legislación al respecto y con instituciones relacionadas específicamente a los padres y familiares y a los ciudadanos en general. La seguridad de los niños es tarea de adultos, protegerlos ante cualquier forma de abuso corresponde al entorno que le rodea. Los Derechos de los menores deben prevalecer por encima de los de cualquier persona adulta, para ello, todos los esfuerzos a realizar ante un posible caso de abuso deben estar dirigidos a una mínima intervención, agilización, coordinación y, sin lugar a dudas, a obtener todas las garantías procesales que la situación requiera.

En segundo lugar conviene indicar que este artículo se va a centrar exclusivamente en el procedimiento de entrevista a menores en casos de delitos contra la libertad sexual. En este sentido es necesario recordar en este momento cuáles son los delitos contra la libertad sexual que recoge el ordenamiento jurídico español (título VIII del Código Penal Español):

2 La victimización es el proceso que padece una persona tras el suceso de un hecho traumático (Tamarit, 2006), variando de formas muy diferentes de unos individuos a otros. Khüne (1986) acuñó el término victimización secundaria para referirse al conjunto total de las agresiones psíquicas sufridas por la víctima en la relación con los diferentes profesionales e instituciones del proceso.

Capítulo	*Delito*	*Artículos*	*Texto*
I	*AGRESIÓN SEXUAL*	*178*	*El que atentare contra la libertad sexual de otra persona, utilizando violencia o intimidación, será castigado como responsable de agresión sexual con la pena de prisión de uno a cinco años.*
		179	*Cuando la agresión sexual consista en acceso carnal por vía vaginal, anal o bucal, o introducción de miembros corporales u objetos por alguna de las dos primeras vías, el responsable será castigado como reo de violación con la pena de prisión de seis a 12 años.*
		180.1	*Las anteriores conductas serán castigadas con las penas de prisión de cinco a diez años para las agresiones del artículo 178, y de 12 a 15 años para las del artículo 179, cuando concurra alguna de las siguientes circunstancias:* *1. Cuando la violencia o intimidación ejercidas revistan un carácter particularmente degradante o vejatorio.* *2. Cuando los hechos se cometan por la actuación conjunta de dos o más personas.* *3. Cuando la víctima sea especialmente vulnerable, por razón de su edad, enfermedad, discapacidad o situación, salvo lo dispuesto en el artículo 183.* *4. Cuando, para la ejecución del delito, el responsable se haya prevalido de una relación de superioridad o parentesco, por ser ascendiente, descendiente o hermano, por naturaleza o adopción, o afines, con la víctima.* *5. Cuando el autor haga uso de armas u otros medios igualmente peligrosos, susceptibles de producir la muerte o alguna de las lesiones previstas en los artículos 149 y 150 del Código Penal, sin perjuicio de la pena que pudiera corresponder por la muerte o lesiones causadas.*
		180.2	*Si concurrieren dos o más de las anteriores circunstancias, las penas previstas en este artículo se impondrán en su mitad superior.*
II	*ABUSO SEXUAL*	*181*	*1. El que, sin violencia o intimidación y sin que medie consentimiento, realizare actos que atenten contra la libertad o indemnidad sexual de otra persona, será castigado como responsable de abuso sexual, con la pena de prisión de uno a tres años o multa de 18 a 24 meses.* *2. A los efectos del apartado anterior, se consideran abusos sexuales no consentidos los que se ejecuten sobre personas que se hallen privadas de sentido o de cuyo trastorno mental se abusare, así como los que se cometan anulando la voluntad de la víctima mediante el uso de fármacos, drogas o cualquier otra sustancia natural o química idónea a tal efecto.* *3. La misma pena se impondrá cuando el consentimiento se obtenga prevaliéndose el responsable de una situación de superioridad manifiesta que coarte la libertad de la víctima.* *4. En todos los casos anteriores, cuando el abuso sexual consista en acceso carnal por vía vaginal, anal o bucal, o introducción de miembros corporales u objetos por alguna de las dos primeras vías, el responsable será castigado con la pena de prisión de cuatro a diez años.* *5. Las penas señaladas en este artículo se impondrán en su mitad superior si concurriere la circunstancia 3.ª o la 4.ª , de las previstas en el apartado 1 del artículo 180 del código penal.*

		182	*1. El que, interviniendo engaño, realice actos de carácter sexual con persona mayor de 13 años y menor de 16, será castigado con la pena de prisión de uno a dos años, o multa de 12 a 24 meses.* *2. Cuando los actos consistan en acceso carnal por vía vaginal, anal o bucal, o introducción de miembros corporales u objetos por alguna de las dos primeras vías, la pena será de prisión de dos a seis años. La pena se impondrá en su mitad superior si concurriera la circunstancia 3.ª, o la 4.ª, de las previstas en el artículo 180.1 del código penal.* *– este artículo agrava los actos sexuales recogidos en el artículo 181 cuando exista acceso carnal por alguna de las vías referidas*
II bis	*DE LOS ABUSOS Y AGRESIONES SEXUALES A MENORES DE 13 AÑOS*	*183*	*1. El que realizare actos que atenten contra la indemnidad sexual de un menor de 13 años será castigado como responsable de abuso sexual a un menor con la pena de prisión de dos a seis años.* *2. Cuando el ataque se produzca con violencia o intimidación el responsable será castigado por el delito de agresión sexual a un menor con la pena de cinco a diez años de prisión.* *3. Cuando el ataque consista en acceso carnal por vía vaginal, anal o bucal, o introducción de miembros corporales u objetos por alguna de las dos primeras vías, el responsable será castigado con la pena de prisión de ocho a 12 años, en el caso del apartado 1 y con la pena de 12 a 15 años, en el caso del apartado 2.* *4. Las conductas previstas en los tres números anteriores serán castigadas con la pena de prisión correspondiente en su mitad superior cuando concurra alguna de las siguientes circunstancias:* *a. Cuando el escaso desarrollo intelectual o físico de la víctima la hubiera colocado en una situación de total indefensión y, en todo caso, cuando sea menor de cuatro años.* *b. Cuando los hechos se cometan por la actuación conjunta de dos o más personas.* *c. Cuando la violencia o intimidación ejercidas revistan un carácter particularmente degradante o vejatorio.* *d. Cuando, para la ejecución del delito, el responsable se haya prevalido de una relación de superioridad o parentesco, por ser ascendiente, o hermano, por naturaleza o adopción, o afines, con la víctima.* *e. Cuando el autor haya puesto en peligro la vida del menor.* *f. Cuando la infracción se haya cometido en el seno de una organización o de un grupo criminales que se dedicaren a la realización de tales actividades.* *5. En todos los casos previstos en este artículo, cuando el culpable se hubiera prevalido de su condición de autoridad, agente de esta o funcionario público, se aplicará, además, la pena de inhabilitación absoluta de seis a 12 años.* *BIS: El que a través de Internet, del teléfono o de cualquier otra tecnología de la información y la comunicación contacte con un menor de 13 años y proponga concertar un encuentro con el mismo a fin de cometer cualquiera de los delitos descritos en los artículos 178 a 183 y 189, siempre que tal propuesta se acompañe de actos materiales encaminados al acercamiento, será castigado con la pena de uno a tres años de prisión o multa de 12 a 24 meses, sin perjuicio de las penas correspondientes a los delitos en su caso cometidos. Las penas se impondrán en su mitad superior cuando el acercamiento se obtenga mediante coacción, intimidación o engaño.*

III	*DEL ACOSO SEXUAL*	*184*	*1. El que solicitare favores de naturaleza sexual, para sí o para un tercero, en el ámbito de una relación laboral, docente o de prestación de servicios, continuada o habitual, y con tal comportamiento provocare a la víctima una situación objetiva y gravemente intimidatoria, hostil o humillante, será castigado, como autor de acoso sexual, con la pena de prisión de tres a cinco meses o multa de seis a diez meses.* *2. Si el culpable de acoso sexual hubiera cometido el hecho prevaliéndose de una situación de superioridad laboral, docente o jerárquica, o con el anuncio expreso o tácito de causar a la víctima un mal relacionado con las legítimas expectativas que aquella pueda tener en el ámbito de la indicada relación, la pena será de prisión de cinco a siete meses o multa de 10 a 14 meses.* *3. Cuando la víctima sea especialmente vulnerable, por razón de su edad, enfermedad o situación, la pena será de prisión de cinco a siete meses o multa de 10 a 14 meses en los supuestos previstos en el apartado 1, y de prisión de seis meses a un año en los supuestos previstos en el apartado 2 de este artículo.*
IV	*DE LOS DELITOS DE EXHIBICIONISMO Y PROVOCACIÓN SEXUAL*	*185*	*El que ejecutare o hiciere ejecutar a otra persona actos de exhibición obscena ante menores de edad o incapaces, será castigado con la pena de prisión de seis meses a un año o multa de 12 a 24 meses.*
		186	*El que, por cualquier medio directo, vendiere, difundiere o exhibiere material pornográfico entre menores de edad o incapaces, será castigado con la pena de prisión de seis meses a un año o multa de 12 a 24 meses.*
V	*PROSTITUCIÓN Y CORRUPCIÓN DE MENORES*	*187*	*El que ejecutare o hiciere ejecutar a otra persona actos de exhibición obscena ante menores de edad o incapaces, será castigado con la pena de prisión de seis meses a un año o multa de 12 a 24 meses.*
		188	*1. El que determine, empleando violencia, intimidación o engaño, o abusando de una situación de superioridad o de necesidad o vulnerabilidad de la víctima, a persona mayor de edad a ejercer la prostitución o a mantenerse en ella, será castigado con las penas de prisión de dos a cuatro años y multa de 12 a 24 meses. En la misma pena incurrirá el que se lucre explotando la prostitución de otra persona, aun con el consentimiento de la misma.* *2. Si las mencionadas conductas se realizaran sobre persona menor de edad o incapaz, para iniciarla o mantenerla en una situación de prostitución, se impondrá al responsable la pena de prisión de cuatro a seis años.* *3. El que lleve a cabo la conducta prevista en el apartado anterior, siendo la víctima menor de 13 años será castigado con la pena de prisión de cinco a diez años.* *4. Se impondrán las penas previstas en los apartados anteriores en su mitad superior, en sus respectivos casos, cuando concurra alguna de las siguientes circunstancias:* *a. Cuando el culpable se hubiera prevalido de su condición de autoridad, agente de esta o funcionario público. En este caso se aplicará, además, la pena de inhabilitación absoluta de seis a 12 años.* *b. Cuando el culpable perteneciere a una organización o grupo criminales que se dedicaren a la realización de tales actividades.* *c. Cuando el culpable hubiere puesto en peligro, de forma dolosa o por imprudencia grave, la vida o salud de la víctima.* *5. Las penas señaladas se impondrán en sus respectivos casos sin perjuicio de las que correspondan por las agresiones o abusos sexuales cometidos sobre la persona prostituida.*

		189	*1. Será castigado con la pena de prisión de uno a cinco años: a. El que captare o utilizare a menores de edad o a incapaces con fines o en espectáculos exhibicionistas o pornográficos, tanto públicos como privados, o para elaborar cualquier clase de material pornográfico, cualquiera que sea su soporte, o financiare cualquiera de estas actividades o se lucrare con ellas. b. El que produjere, vendiere, distribuyere, exhibiere, ofreciere o facilitare la producción, venta, difusión o exhibición por cualquier medio de material pornográfico en cuya elaboración hayan sido utilizados menores de edad o incapaces, o lo poseyere para estos fines, aunque el material tuviere su origen en el extranjero o fuere desconocido.* *2. El que para su propio uso posea material pornográfico en cuya elaboración se hubieran utilizado menores de edad o incapaces, será castigado con la pena de tres meses a un año de prisión o con multa de seis meses a dos años.* *3. Serán castigados con la pena de prisión de cinco a nueve años los que realicen los actos previstos en el apartado 1 de este artículo cuando concurra alguna de las circunstancias siguientes:* *a. Cuando se utilicen a niños menores de 13 años.* *b. Cuando los hechos revistan un carácter particularmente degradante o vejatorio.* *c. Cuando los hechos revistan especial gravedad atendiendo al valor económico del material pornográfico.* *d. Cuando el material pornográfico represente a niños o a incapaces que son víctimas de violencia física o sexual.* *e. Cuando el culpable perteneciere a una organización o asociación, incluso de carácter transitorio, que se dedicare a la realización de tales actividades.* *f. Cuando el responsable sea ascendiente, tutor, curador, guardador, maestro o cualquier otra persona encargada, de hecho o de derecho, del menor o incapaz.* *4. El que haga participar a un menor o incapaz en un comportamiento de naturaleza sexual que perjudique la evolución o desarrollo de la personalidad de este, será castigado con la pena de prisión de seis meses a un año.* *5. El que tuviere bajo su potestad, tutela, guarda o acogimiento a un menor de edad o incapaz y que, con conocimiento de su estado de prostitución o corrupción, no haga lo posible para impedir su continuación en tal estado, o no acuda a la autoridad competente para el mismo fin si carece de medios para la custodia del menor o incapaz, será castigado con la pena de prisión de tres a seis meses o multa de seis a 12 meses.* *6. El ministerio fiscal promoverá las acciones pertinentes con objeto de privar de la patria potestad, tutela, guarda o acogimiento familiar, en su caso, a la persona que incurra en alguna de las conductas descritas en el apartado anterior.* *7. Será castigado con la pena de prisión de tres meses a un año o multa de seis meses a dos años el que produjere, vendiere, distribuyere, exhibiere o facilitare por cualquier medio material pornográfico en el que no habiendo sido utilizados directamente menores o incapaces, se emplee su voz o imagen alterada o modificada.*

Tabla 1. Delitos contra la libertad sexual.

2. LA ENTREVISTA COMO TÉCNICA DE INVESTIGACIÓN

Ciencias como la Psicología o la Sociología comenzaron a utilizar la entrevista como técnica de investigación a finales de los años 30. Desde esa época se viene utilizando para recoger datos e informar sobre la realidad (Bingham y Moore, 1961). Es la técnica por excelencia cuando se pretende acceder a información que no se ha presenciado, especialmente cuando no existen otros medios como pueden ser los circuitos cerrados de seguridad o las cámaras de videovigilancia. Cuando se habla de entrevista, se hace referencia a un sistema de comunicación interpersonal que integra tanto a un entrevistador como a un entrevistado. El primero deberá tener especial cuidado en no influenciar, contaminar o determinar el discurso del segundo. Aunque el entrevistador deba enfocar y dirigir la conversación para conseguir los objetivos que se ha propuesto, éste debe mantenerse siempre en un segundo plano, evitando siempre el protagonismo, y permitir hablar y explicarse al entrevistado. El fin último que se persigue con esta técnica de investigación es la recogida de la información de la forma más objetiva posible sin que igualmente el entrevistador sea contagiado por el estado emocional, sensaciones o sentimientos del entrevistado. A la hora de entrevistar, en general, no resulta difícil encontrarse con discursos exagerados, misivas, tendencia a ocultar información, etc. A veces existen personas que informan sobre su propia interpretación de lo que pasó, otras que, movidas por intereses personales, contaminan el testimonio a su favor, etc. Estas y otras circunstancias dificultan con frecuencia la tarea del entrevistador y, en muchas ocasiones, les lleva a realizar un análisis y valoración de fuentes, comparando la información obtenida con la de otras entrevistas y complementarla con las proporcionadas por otras técnicas de recogida (González, 2006). A parte de las dificultades mencionadas, la persona que realiza la entrevista se podrá encontrar con otra serie de dificultades añadidas, entre ellas por ejemplo destaca por un lado la voluntad de colaboración del entrevistado, es decir la actitud para compartir lo que ha vivido o presenciado. El otro gran obstáculo que puede existir se debe a la propia dificultad de recordar todo lo que de una u otra forma se ha ido viviendo, ya que, como se verá más adelante, no todo lo que se ve o se oye, se procesa en el cerebro. Para intentar solventar el primer obstáculo, el entrevistador deberá poner en práctica diferentes estrategias, motivaciones o habilidades de comunicación para intentar convencer al entrevistado de la importancia de su testimonio. En el segundo caso, para hacer consciente lo vivido y poder expresarlo de forma clara y próxima a la realidad, se deberá hacer uso de otra serie de técnicas con mayor nivel de complejidad. La memoria, la percepción y la atención son los procesos cerebrales superiores más importantes que se ponen en marcha, tanto en los momentos de almacenamiento como en la evocación de los recuerdos.

3. LIMITACIONES DEL TESTIMONIO

En primer lugar conviene dar una definición sobre el testimonio, tratándose éste de una de las principales pruebas judiciales para decidir la credibilidad de los hechos. Es por tanto la declaración de un testigo cuando afirma algo y asegura que tiene conocimiento verdadero, ya que lo ha presenciado o lo ha vivenciado por él mismo. Pero, para que un testigo tenga conocimiento y pueda llegar a afirmar que ha presenciado o vivido algo, debe tener conservados ciertos procesos psicológicos que están potentemente implicados en el testimonio. Por este motivo, a la hora de emitir una decisión sobre el testimonio, se han de conocer las características de estos procesos.

Lo primero que es preciso indicar antes de comentar los errores o limitaciones de cerebros normales, es que la mente es una maquina imperfecta e incompleta. El cerebro no funciona como una cámara de vídeo y reproduce la realidad de la misma manera que la ha vivido o experimentado previamente, sino que va reconstruyendo constantemente la realidad. Esto tiene gran importancia al hablar de la recogida del testimonio, ya que al recordar hechos pasados las personas se enfrentan a que procesos básicos como la memoria, la percepción o la atención se vean sujetos a limitaciones que les hacen vulnerables e influenciables, con lo que inevitablemente todos los testimonios serán incompletos y presentarán inexactitudes (González, 2006). Como se apuntaba anteriormente, no por estar presente en un escenario eso significa que la persona vaya a ser capaz de describir con precisión todos los detalles que rodean ese escenario (quiénes y dónde estaban allí, cómo eran, de qué color eran su abrigo, cuántos coches había y qué matrículas tenían, por ejemplo…). Del mismo modo, es preciso indicar que serviría de poco el presionar o hacer uso de técnicas como la hipnosis para "ayudar a recordar", puesto que reiterando lo comentado previamente, si no se procesa la información esta no entra en el cerebro y técnicas como las mencionadas pueden dar resultados contraindicados en la investigación, como que el entrevistado dé una respuesta inventada para salir de la situación.

Por el contrario, sí se puede ayudar a las personas a recordar, a facilitarles acceder a sus recuerdos, para ello es fundamental establecer un buen clima de *rapport*, buscar espacios tranquilos, guiar con "pistas" que activen el acceso a la información guardada, incluso utilizar otro tipo de técnicas como las que incluye la entrevista cognitiva: instauración de contexto, cambio de perspectiva, cambio de orden. La entrevista cognitiva ha demostrado ser eficaz en diferentes países, con diferentes tipos de testigos (niños, adultos o personas mayores) y diferentes intervalos temporales entre el evento a recordar y la entrevista, tanto en laboratorios como en estudios de campo (Fisher, Milne y Bull, 2011). Para conseguir esto es preciso utilizar las habilidades básicas de comunicación (parafrasear, escuchar activamente, reducir incertidumbre, animar, resumir…).

Finalmente es útil indicar que, a la hora de llevar a cabo una entrevista de investigación, es preciso que esta se haga cuanto antes, en el mínimo tiempo posible. El cerebro tiende automáticamente a reconstruir información, como respuesta a su intolerancia por los espacios en blanco, rellenando huecos para dar coherencia al contenido. Esto último tiene que ver con el concepto de las Falsas Memorias (Loftus, 2003; Roediger, Watson, McDermott y Gallo, 2001). Se trata de un fenómeno muy estudiado dentro de la Psicología del Testimonio y hace referencia a la distorsión de la información inconscientemente. Las personas desarrollan recuerdos vividos que nunca antes han presenciado o experimentado. A veces es también llamado pseudomemoria o ilusión de memoria. A diferencia de las mentiras, la gente que tiene falsas memorias cree de manera genuina que estas han sucedido cuando realmente nunca lo han vivido (Zhu, 2010).

Por todo esto, el objetivo de la entrevista no es otro que el obtener información precisa, confiable y completa, ya que adquiere un valor fundamental como prueba en el proceso de investigación criminal.

4. ENTREVISTA A MENORES VÍCTIMAS

4.1. PRINCIPIOS BÁSICOS DE ACTUACIÓN

Antes de exponer el protocolo de actuación que la SACD sigue cuando hay que tomar manifestación a un menor, es preciso contemplar cuáles son los principios básicos de actuación, señalando el total respeto que se debe seguir en la actuación policial:

1. Protección: La actuación policial siempre irá encaminada a la protección absoluta del interés superior del menor.
2. Coordinación de las instituciones que intervienen en la investigación. La mayoría de los abusos suceden en ambientes ocultos, lejos de los demás, siendo infrecuente la presencia de testigos, por lo que el testimonio de la víctima es la prueba fundamental en la investigación de los hechos. Por esta razón resulta muy importante trabajar de manera coordinada todos los intervinientes en el proceso.
3. Actuación inmediata: tan pronto como se detecta la situación de abuso o maltrato, el objetivo es evitar la dilatación de los procedimientos, teniendo en cuenta que el tiempo siempre es contraproducente en términos del testimonio.
4. Mínima intervención: Se trata de que los menores eviten ser sometidos a actuaciones repetitivas y reiteradas sobre los mismos hechos. Hay que respetar la preeminencia del procedimiento judicial, con garantía de los principios de contradicción e inmediación de las pruebas.

A continuación se va a exponer cuál es el procedimiento de actuación de los agentes policiales de la SACD, desde que se tiene conocimiento de unos hechos hasta que se emite un informe destinado a la Autoridad Judicial.

4.2. PRIMERAS ACTUACIONES

Tan pronto como se tiene conocimiento de un posible hecho delictivo relacionado con los delitos vistos en el punto 1.2, y donde hay menores de edad[3], lo más importante es la recopilación de toda la información sobre los supuestos hechos (diligencias policiales, entrevista/s de los investigadores, identificación de lugares, de personal relacionado con el caso, entrevistas con otros profesionales y/o historias o antecedentes médicos, psicológicos o policiales). El objetivo de este punto es disponer de toda la información posible para poder planear una entrevista bien hecha y eficaz, evitando precipitaciones inoportunas o el tener que volver a repetir parte de la entrevista, conviene dedicarle un tiempo generoso a esta fase como garantía de la efectividad cuando se haga la entrevista. Igualmente habrá que preparar las preguntas indispensables, tanto a la supuesta víctima como a la familia, cuidando la forma y el contenido de las mismas.

En este momento, hay que asesorar muchas veces tanto a los investigadores que llevan el caso como a los padres o familiares que son con los que hay que hablar para programar la entrevista. Este asesoramiento irá siempre encaminado a tranquilizar,

3 Los agentes de la SACD interviene con menores de hasta 8 o 9 años de edad. Mayores de esta edad se encargarían los agentes del EMUME de la Guardia Civil.

explicar el procedimiento y especialmente a recalcar que no se comente nada de los supuestos hechos con los menores de edad.

Seguidamente hay que planificar la entrevista, el lugar, la hora, supervisar los medios técnicos de los que se dispone así como el material de apoyo. Conviene indicar que al entrevistar a un menor se debe evitar interrumpir sus rutinas, elegir un espacio sin distracciones, se deben programar descansos y detallar con detenimiento las secuencias de los aspectos a explorar.

En relación al entorno físico es importante destacar los siguientes aspectos:

Un ambiente acondicionado especialmente para el desarrollo de la entrevista debe reunir como propiedades principales la ausencia de ruidos e interrupciones de ningún tipo. El menor debe tener y sentir la seguridad de que nadie más entrará por la puerta, ni llamarán, ni oirá voces ni ruidos externos que puedan desconcentrarle durante la entrevista.

Es preciso apuntar que los agentes de la SACD, en la mayoría de los casos, acuden a los domicilios familiares a entrevistarse tanto con los familiares como con las propias víctimas, esto supone una ventaja en términos de comodidad para la familia y, lo que es más importante, de cara al testimonio, ya que se trata de un ambiente donde los menores se sienten cómodos, en su propio espacio. Si bien es cierto que en algunas ocasiones esta práctica no se puede llevar a cabo por circunstancias sobrevenidas, en ese caso se opta por espacios sociales (ayuntamientos, centros escolares, sociales) o las propias dependencias policiales, lo ideal sería contar con una sala especialmente acondicionada, pero habitualmente hay que adaptarse a las circunstancias del entorno siempre siguiendo los siguientes criterios:

- Decoración de la sala: Será agradable a la vista, placentera, sencilla, iluminada, adecuada para las diferentes edades de las posibles víctimas y libre de ruidos. Evitando salas que contengan mucho material y eligiendo siempre aquellas que no tengan ningún tipo de “distractor”, con la excepción de material de dibujo, de escritura, que serán utensilios de obligada existencia en la sala, ya que según la situación pintar o escribir puede ayudar a la víctima a relajarse y encontrase más cómoda. Otros harán uso de juguetes que estarán fuera del alcance de la vista, siendo introducidos por el profesional cuando lo considere oportuno para el relato del testimonio, fundamentalmente será aplicado con menores de edad pre-escolar y escolar.
- Medios técnicos: Contar con una instalación acondicionada de sistema de circuito cerrado de televisión en la propia sala, hará de la grabación algo mucho menos frío e intimidante para el menor durante la exposición de los hechos. De no ser así, se hará uso de la grabación a través de cámara, haciendo participe al menor tanto en la instalación como en los primeros minutos de grabación. Conviene recordar que en el caso que los agentes se desplacen al domicilio familiar siempre irán previstos de ella y grabarán todo lo realizado con los menores, siempre a disposición de la Autoridad Judicial.
- Otros: Para conseguir mayor comodidad y no entrar en interrupciones innecesarias ni abandonos del menor, contar en la misma sala con botellas de agua y otros utensilios que harán del entorno algo más cercano y práctico.

Finalmente, y en relación **con los objetivos de la entrevista**, estos siempre irán encaminados a conseguir la siguiente información:

1. Importancia de obtener información en cantidad y calidad.
2. Conseguir que el menor relate quién ha hecho qué, dónde, cuándo, con qué, con la mayor cantidad de detalles y pruebas para la investigación policial.

Estos objetivos son de extrema importancia ya que, como se comentó anteriormente, cuando se habla por ejemplo de abusos sexuales, probablemente no se cuente con otro tipo de indicios (físicos, biológicos, testificales….).

4.3. ENTREVISTA A DENUNCIANTES

Con denunciantes se hace referencia a los padres, tutores legales o aquellos familiares o allegados que quieran interponer denuncia porque sospechan de unos hechos delictivos. En esta entrevista se explorarán todos los detalles de los hechos denunciados: cómo fue la revelación del menor, si fue espontánea u obedeció a preguntas encaminadas a los hechos, cuál fue el contexto en el que se produjo y, especialmente, se mostrará interés en cómo fue la reacción del entorno a los hechos. Se obtendrá información igualmente sobre la relación entre el presunto autor/a de los hechos y el menor, la relación con la familia y la posible existencia de intereses o ganancias secundarias a la hora de interponer la denuncia. Un aspecto importante de este encuentro es obtener información sobre los lugares o momentos de ocurrir los hechos, es decir la oportunidad. Finalmente se harán preguntas con el objetivo de conseguir información sobre el contexto y la estructura familiar, social y cultural.

Seguidamente, y en relación con el menor, se preguntará sobre las rutinas familiares y/o escolares, los posibles cambios en el comportamiento, los conocimientos sexuales del menor y las palabras que utiliza para designar los órganos sexuales. Se les pedirá que cuenten un relato indubitado para poder crear la línea base con el menor sobre algún acontecimiento llamativo (un cumpleaños, una fiesta, una excursión), y se les explicará el procedimiento de entrevista solicitando su consentimiento para la exploración del menor sin su presencia y poder utilizar la grabación en vídeo.

4.4. ENTREVISTA AL MENOR

A continuación se va a describir el protocolo de entrevista seguido por los agentes de la SACD, indicando que está basado en el protocolo NICH versión 2007 (Lamb, Orbach, Hershkowitz, Esplin y Horowitz) y en el protocolo de Entrevista Forense Estado de Michigan (Poole & Lamb, 1998).

En relación con los entrevistadores es preciso mencionar que la SACD cuenta con agentes doctores y licenciados en Psicología y en Criminología, con formación específica en testimonio. Normalmente suelen acudir dos agentes, actuando uno como entrevistador principal, que dirige la entrevista, y el otro como auxiliar, tomando notas, realizando preguntas adicionales y controlando la cámara de grabación en todo momento.

Si se diera el caso que el menor precisara de alguna persona de confianza durante la entrevista, esta permanecerá fuera del campo de visión del menor, estará solo los

primeros momentos y recibirá claras instrucciones sobre cuál debe ser su actitud y conducta durante la entrevista.

Conviene considerar algunos aspectos a tener en cuenta en estos momentos: los entrevistadores, aunque suelen ser agentes policiales, irán siempre vestidos de paisano. Tendrán especial cuidado con aspectos claves de la comunicación no verbal (gestos, posturas, contacto, tono, velocidad del habla), intentado mantener siempre una postura lo más objetiva posible, sin reforzar al entrevistado, sin mostrar signos de alarma, asombro o prestar atención más a unos detalles que a otros. El objetivo inicial principal es establecer un clima de confianza con el menor, depositando seguridad e intimidad. En relación a la construcción de este *rapport* conviene recordar que: consiste en una relación positiva entre el entrevistador/a y el entrevistado/a que genera el 'clima' en que se desarrollará el resto del proceso de valoración y contribuye a aumentar la cantidad y la exactitud de la información suministrada (Boggs y Eyberg, 1990). Algunos consejos para un buen establecimiento del *rapport* según Sattler (1998) son:

- Llamar al niño por su nombre,
- Prestar una total atención,
- Mostrar gran interés por lo que cuenta,
- Dar apoyo y seguridad,
- Escuchar de manera abierta, sin prejuicios ni gestos,
- Utilizar un tono cálido y expresivo,
- Mantener una actitud relajada, atenta y espontánea,
- Tomar contacto visual de forma apropiada,
- Tener en cuenta la posible ansiedad del menor.

Lo primero que se activa es el equipo de grabación, para ello se dispone de un espacio donde se pueda colocar el trípode, cerca de una toma de electricidad, y se empiezan a hacer los primeros acercamientos de la cámara con el menor para que este se habitúe a ella. Seguidamente se registran los datos aportados por los menores (edad, lugar, fecha, hora, personas presentes…).

4.4.1. Etapas de la entrevista

Se pueden establecer las siguientes fases:

1. Presentación: donde el entrevistador se presenta y comenta en un lenguaje comprensible para el niño el objetivo de la entrevista.
2. Reglas de la entrevista: Se recalca en esta fase las siguientes reglas:
   - Importancia de decir solo la verdad, mientras se van poniendo ejemplos.
   - Se le da permiso para responder "no me acuerdo" o "no lo sé" en lugar de inventar.
   - Si no entiende algo, se le da permiso para decir "no lo entiendo" y el entrevistador se asegura que entiende estos conceptos.

- Se le anticipará posible repetición de preguntas.
- Se enfatiza su protagonismo.
- Se le informa que se pedirán detalles sobre lo que diga.
- Se debe siempre tranquilizar, desculpabilizar y asegurar la confidencialidad en un lenguaje comprensible por los menores.
- Se debe advertir que posiblemente habrá temas de los que no quiera hablar.

3. Evaluación de las capacidades: En esta etapa se tratará de dar respuestas a las siguientes preguntas relacionadas con las capacidades, aspecto fundamental y previo a la recogida de cualquier testimonio. En general se tratará de obtener información sobre si el menor es capaz de orientarse espacial y temporalmente, si puede identificar lugares y personas, si sabe nombrar las diferentes partes del cuerpo humano, si puede identificar objetos y para qué sirven, si sabe contar, si es fácilmente influenciable o sugestionable, si distingue entre lo real y la fantasía o si introduce fantasías en su discurso, etc.… Para poder explorar estas capacidades los agentes suelen contar con diferentes dibujos auxiliares que hacen que el niño ofrezca información a las preguntas anteriores formuladas.

4. Relato libre: en esta fase se le suele pedir que narre un relato neutro, que anteriormente se ha comentado con los denunciantes, para explorar su memoria episódica, introducción de detalles, ritmo y cadencia del relato, etc. Con esta información se suele crear una línea base a utilizar luego para compararla con los datos que nos cuente sobre los supuestos hechos.

5. Introducción del tema: Importante en esta fase observar si el niño ha introducido el tema espontáneamente o ha sido preciso utilizar preguntas más concretas. El objetivo es obtener un relato lo más libre posible, animar constantemente al niño a que continúe con preguntas como las que siguen “¿y qué más?”, “¿y después qué paso?”. Conviene resaltar la paciencia que debe tener todo investigador cuando se trabaje con niños, ya que suelen ir a otro ritmo diferente al de los adultos, por ello será importante ir reforzando tanto el esfuerzo como el rendimiento, ir pidiendo que resuma de vez en cuando e introducir algunas preguntas “trampas” para ver cómo los menores responden a este tipo de situaciones, es decir, si incorporan las trampas a sus discurso o las “debaten”. Igualmente importante en esta fase será explorar hipótesis alternativas que puedan explicar los hechos e indagar los conocimientos sexuales de los menores. Al finalizar esta etapa se debe ser capaz de explicar varias preguntas: qué ha pasado, a quién y por parte de quién, cuántas veces, la duración, cómo ocurrió y con qué parte/s del cuerpo, si hubo daño, qué tuvo que hacer él, qué le decía mientras tanto, cuáles eran las circunstancias dónde sucedieron los hechos, si había más personas que presenciaron los hechos, si se lo ha visto hacer a alguien más, si le dijeron que no lo contase, si hubo regalos, amenazas, etc…

6. Preguntas y aclaraciones: Esta fase está diseñada para el establecimiento de aquellas preguntas o interrogantes que no han quedado claras a lo largo de la entrevista.

7. Cierre: Se debe alabar siempre el esfuerzo realizado, acabando con un tema neutro, como puede ser hablar de las vacaciones o de dibujos animados.

   En relación a los padres habrá que darle información a modo de *feedback* sobre cómo ha ido la entrevista y qué se ha obtenido del testimonio del menor, resolviendo sus dudas y estableciendo unas pautas a seguir con el menor. Con respecto a los investigadores, se les comunicará las impresiones y primeros resultados obtenidos, se propondrán propuestas de investigación, así como recomendaciones operativas a la hora de proceder.

4.4.2. Aspectos a evitar durante la entrevista a los menores

Durante la entrevista es preciso evitar los aspectos que se relatan más abajo, puesto que, además de poder convertirse en limitaciones a la hora de defender el informe en una futura vista oral, se convierten en verdaderos problemas a la hora de esclarecer los hechos:

- Centrar la entrevista solo en la hipótesis del abuso, sin explorar alternativas. Esta afirmación responde a la idea de que “uno termina encontrando aquello que busca”. En esta fase de la investigación el entrevistador debe ser lo más neutral y objetivo posible, se deben explorar todas las hipótesis posibles que puedan explicar los supuestos hechos. En ocasiones, se ha podido malinterpretar las palabras o gestos de los menores, o incluso puede haber ganancias secundarias por parte de los denunciantes que es preciso considerar.

- Preguntar repetidamente hasta obtener la respuesta deseada. Recordemos que los menores normalmente piensan que los mayores, por el mero hecho de ser adulto, saben todas las respuestas. Si le formulamos una misma pregunta en varias ocasiones, al final el menor tenderá a cambiar su respuesta, porque pensará que lo está haciendo mal y de esta manera contentará al entrevistador y terminará con esa pregunta. Durante la entrevista se puede repetir al niño que “nosotros no estábamos allí y es muy importante que nos cuente la verdad”, y que si le preguntamos algo varias veces es porque no nos queda claro y tenemos que reiterar la pregunta.

- Reforzar selectivamente determinadas respuestas. Muchos entrevistadores que se guían con una sola hipótesis (bien la del abuso, o la del no abuso), centran sus preguntas en determinar éste y van reforzando, bien directamente o a través de la comunicación no verbal, a los menores en esa dirección. Esto es contraproducente de cara a la defensa del informe el día del juicio y puede traer problemas a la hora de la exactitud del testimonio.

- Emplear muñecos anatómicamente correctos. Es decir, muñecos con características sexuales. Esta práctica puede ser problemática en aquellos casos donde los niños tan pronto como se les dan los juguetes empiezan a jugar con ellos, y muchas veces al final terminan introduciendo las piezas más sobresalientes en los agujeros o huecos que presentan los muñecos. De cara a la interpretación de estos gestos puede ser problemático y peligroso en la defensa del testimonio.

- Inducir estereotipos negativos. Hay que recordar, en este punto, que el investigador siempre es una persona neutra, que utilizará un lenguaje neutro y que

intentará ser lo más objetivo posible, evitando etiquetas como por ejemplo “el malo”, cuando se habla del supuesto autor.

- Utilizar sobornos y/o amenazas
- Preguntas cerradas e intervenciones sugerentes. Las preguntas cerradas limitan el testimonio, puesto que ofrecen a los menores posibilidades muy reducidas para responder. En este sentido, lo ideal y recomendado es utilizar el relato amplio, dando ligeras indicaciones al menor sobre la dirección de su discurso, reforzando y animando a que nos cuente más.
- Empleo inadecuado de la autoridad. Los menores tienen que ver a los entrevistadores como personas de confianza a los que contarle “algo” que ha pasado, el uso de la autoridad esta absolutamente contraindicado, corriendo el riesgo de que el menor cuente un falso testimonio, con el objetivo de “salir cuanto antes del paso”.

4.4.3. Otros aspectos importantes

En esta fase de la entrevista, hay otros conceptos que son importantes de cara a la recogida del testimonio:

- No dar nada por supuesto. Un entrevistador no puede “leer entrelíneas” o interpretar gestos o “suponer lo que están diciendo los menores”. Debe pedir siempre explicaciones y solicitar muchos detalles. Por ejemplo, si el menor en un momento dice que “le tuvo que chupar”, tenemos que indagar qué significa “chupar” para el menor y, lo que es más importante, que lo represente a ser posible y que ofrezca muchos detalles sobre el propio término.
- Usar frases sencillas. Cuando se habla con personas vulnerables en general y de niños en particular, se debe ajustar el lenguaje en todos los sentidos, siendo uno de ellos la conjugación de las frases. Se deben utilizar frases cortas y sencillas, que el niño las pueda entender sin problemas. En el caso que se tenga que utilizar algún concepto más difícil, el entrevistador se debe asegurar de que el niño ha entendido lo que se le pregunta. De no ser así se corre el riesgo de obtener información sesgada.
- Preguntas una a una. Del mismo modo que en el apartado anterior, las preguntas deben ser sencillas, cortas y formuladas una a una. Es un error muy común de los entrevistadores el hacer más de una pregunta en un mismo interrogante.
- Dar tiempo a responder y tener mucha paciencia. Los niños y las personas vulnerables suelen ir a otro ritmo, necesitando más tiempo para entender, interpretar y responder.
- Los niños, cuando hablan con adultos, están acostumbrados a que sean los mayores quienes dirijan la conversación. El entrevistador hará preguntas abiertas que permitan respuestas amplias y extensas, buscando siempre la mejor manera de profundizar en el tema y poder así ampliar al máximo los detalles del testimonio.

4.4.4. Informe del caso

Finalmente, y como paso último de la exploración, los agentes de la SACD escriben un informe que va dirigido a la Autoridad Judicial o al Fiscal solicitante. En dicho informe constan los antecedentes del caso, las actuaciones y metodología empleada por los psicólogos, los resultados obtenidos de la exploración y, lo que es más importante, la valoración y las conclusiones con la recomendación a los investigadores principales del caso.

5. CONCLUSIONES

La mayoría de los casos con los que se encuentran los agentes de la SACD corresponden con delitos de abusos sexuales a menores de edad, en los que habitualmente no hay lesiones físicas, ni testigos, ni cámaras de grabación, por lo que el único dato probatorio de los hechos es el testimonio del menor. La entrevista se ha convertido en la técnica por excelencia para poder recoger la declaración de la forma menos dañina posible al objeto de evitar la revictimización. Se trata de determinar con esta prueba si la revelación de estos niños tiene indicadores de credibilidad, si los niños distinguen la fantasía de lo que es verdad, sin presiones externas, y en los casos que sean verídicos, tratar de aportar la mayoría de detalles posibles sobre los hechos investigados para ponerlos a disposición, lo antes posible, de la Autoridad Judicial.

REFERENCIAS BIBLIOGRÁFICAS

Alcón, M. F. y De Montalvo, F. (2011) (Coords.). *Los menores en el proceso judicial*. Madrid: Técnos.

Bingam, W. V. y B. V. Moore. (1973). *Cómo entrevistar.* Madrid: Rialp.

Boggs, S. R. Y Eyberg, S. (1990). Interviewing techniques and establishing rapport", en A. M. Greca(ed), *Through the eyes of the child.* Boston: Allyn and Bacon.

Bull, R., Valentine, T. y Williamson, T. (2009). *Handbook of Psychology of Investigative Interviewing: Current Developments and Future Directions*. Chichester: Wiley.

Caso, M., Arch, M., Jarne, A. y Molina, A. (2011). *Guía práctica de exploración de menores*. Madrid: Editorial Jurídica Sepín.

Federación Internacional de Sociedades de la Cruz Roja y de la Media Luna Roja (2010). http://.cruzroja.es

Fisher, R. P., Milne, R., y Bull, R. (2011). Interviewing cooperative witnesses. *Current Directions in Psychological Science*, 20, 16-19.

González A. JL. (2005) "*La Entrevista Cognitiva en la Guardia Civil*". Tesis Doctoral. UNED. Madrid.

González A, JL. (2006). La entrevista Policial. Sin publicar UTPJ.

Kühne, H. H. (1986). Kriminologie: Victimologie der Notzucht. *Juristische Schulung, 5*, 388-394.

Lamb, M. E., Orbach, Y., Hershkowitz, I., Esplin, P. W. y Horowitz, D. (2007). A structured forensic interview protocol improves the quality and informativeness of inves-

tigative interviews with children: A review of research using the NICHD Investigative Interview Protocol. *Child Abuse & Neglect, 31*, 1201-1231.

Lameiras, M. y Orts, E. (2014) (Coords.). Delitos sexuales contra menores. Abordaje psicológico, jurídico y policial. Valencia: Tirant lo Blanch.

Loftus, E. F.(2003). Our changeable memories: Legal and practical implications. *Nature Reviews: Neurosciencience*, 4, 231-234.

Ley Orgánica 10/ 1995, de 23 de noviembre, del Código Penal.

Ley Orgánica 11/ 1999, de 30 de abril, de modificación del Título VIII del Libro II del Código Penal.

Manzanero, A. L. (2010). *Memoria de testigos. Obtención y valoración de la prueba testifical*. Madrid: Pirámide.

Odriozola, E. E., & Zunzunegui, I. J. S. (2008). Guía de buena práctica psicológica en el tratamiento judicial de los niños abusados sexualmente. *International Journal of Clinical and Health Psychology*, *8*(3), 733-749.

Poole, D. A. y Lamb, M.E. (1998). Investigative Interview of children: A Guide for helping professionals. Washington. D.C.

Roediger, H.L., Watson, J.M., McDermott, K.B. y Gallo, D.A. (2001). Factors that determine false recall: A multiple regression analysis. *Psychonomic Bulletin & Review, 8*, 385-407.

Sattler, J.M. (1998). Clinical and Forensic interviewing of children and families. *Guidelines for the mental health, education, paediatric and chlid maltreatment fields*. San Diego, CA: Author.

Simons D J, Chabris C. F, 1999, “Gorillas in our midst: sustained inattentional blindness for dynamic events” *Perception* 28(9) 1059 – 1074.

Sotoca, A., Muñoz, J. M., González, J.L. y Manzanero, A. L. (2013). La prueba preconstituida en casos de abuso sexual infantil: aportaciones desde la psicología jurídica. *La Ley Penal,* 102 . pp. 112-122.

Tamarit, J. (2006). La Victimología: Cuestiones conceptuales y metodológicas. En E. Baca & E. Echeburúa & J.M. Tamarit (Coords.), *Manual de Victimología* (1a.ed., pp. 15-36). Valencia, España: Tirant Lo Blanch.

Zhu B. (2010). Individual differences in false memory from misinformation: Cognitive factors. Psychology Press. 18(5), 543-555

Fecha de recepción: 20/09/2016. Fecha de aceptación: 20/12/2016

LA GUARDIA CIVIL EN PUERTO RICO: CREACIÓN Y ORGANIZACIÓN DE LA INSTITUCIÓN

RAFAEL HERNANDEZ ALONSO

SERVICIO DE ESTUDIOS HISTÓRICOS DE LA GUARDIA CIVIL

RESUMEN

Los primeros proyectos para establecer la Guardia Civil en Puerto Rico se debieron a los capitanes generales Fernando Cotoner y Chacón (1857) y Félix María de Messina (1863), pero estos intentos quedaron paralizados tanto por motivos económicos como por la despreocupación del Gobierno de Madrid por los problemas antillanos. No fue hasta el Grito de Lares de 1868 cuando se puso en evidencia la necesidad de contar con una fuerza de orden público, que vigilara y controlara los nuevos brotes separatistas que pudieran surgir. Un año después, con personal voluntario de los cuerpos de guarnición en la Isla, el capitán general José Laureano Sanz y Posse pondría en marcha la organización provisional de un Tercio de la Guardia Civil. La amalgama de 1871, que unificó los tercios de Ultramar con los peninsulares, supuso la consolidación definitiva de la Institución en la Isla.

Palabras claves: Ultramar, Guardia Civil, Puerto Rico, organización.

ABSTRACT

The first projects to establish the Guardia Civil in Puerto Rico were made by General Captains Fernando Cotoner y Chacón (1857) and Félix María de Messina (1863), but these attemps were abandoned due to economic reasons and the fact that the Government in Madrid was not much interested in the issues of the Antilles. It was in 1868 when the Cry of Lares showed the need to organize a force of public order, which would monitor and control the new separatist outbreaks that may arise. A year later, with volunteers from the army on the island, General Captain José Laureano Sanz y Posse organized an interim Guardia Civil Tercio. The unification of the Ultramar Tercios with Spain Tercios in 1871 was the final consolidation of this institution in Puerto Rico.

Keyword: Overseas, Guardia Civil, Puerto Rico, organization.

1. INTRODUCCIÓN

La presencia de la Guardia Civil en las colonias de Ultramar es una de las cuestiones menos estudiadas de la historia del Cuerpo. Lo publicado sobre el tema se circunscribe principalmente a dos aspectos, por un lado, a la amalgama de 1871 de los tercios de Ultramar con los peninsulares y, por otro, a las vicisitudes de la Guardia Civil en Cuba. Respecto a la Guardia Civil en Puerto Rico, esta siempre ha sido tratada desde un punto de vista marginal, posiblemente debido a que el movimiento insurreccional no alcanzó aquí la importancia que en la vecina Cuba. El teniente Andrés Molinero (1879) y el capitán Miguel Gistau (1907) fueron los primeros autores en

reseñar la historia de la Guardia Civil en la Isla, limitándose los autores posteriores a reproducir lo expuesto por estos dos oficiales del Cuerpo.

En el presente trabajo se van a exponer las distintas fases del proceso de creación y organización de la Guardia Civil en Puerto Rico. La historiografía atribuye erróneamente el primer proyecto de implantar la Guardia Civil en la Isla, el 22 de agosto de 1857, al capitán general José Lemery[1]. En realidad este proyecto se debe a su sucesor Fernando Cotoner que ocupa el cargo en esa fecha[2], por lo que se comenzará con la exposición de este proyecto y el posterior de Félix Messina. A continuación, se desarrollará el proceso de organización provisional del Tercio de Puerto Rico por José Laureano Sanz y su consolidación, al amalgamarse con los tercios peninsulares. Finalizando con el repaso a las reorganizaciones posteriores sufridas por el Tercio hasta su repatriación a España en 1898.

Como fuente principal para la elaboración de este trabajo se ha utilizado la documentación obrante en los archivos Histórico Nacional (AHN), sección de Ultramar e Histórico Militar de Madrid (AHMM), Capitanía General de Puerto Rico.

2. LA CUESTIÓN DEL ORDEN PÚBLICO EN PUERTO RICO EN EL SIGLO XIX

El capitán general, como representante del Gobierno español en Puerto Rico, ejercía todas las competencias de Gobierno, Justicia, Hacienda y Guerra en la colonia. La cuestión del orden público en Puerto Rico no había representado un problema importante para las autoridades locales, siendo suficiente con las instituciones existentes para mantener la tranquilidad en el territorio. Manuel Luengo apunta como factores de esta situación a: la idiosincrasia de la población isleña, la casi inexistencia de población foránea de aluvión, generalmente introductora de delincuencia, y su menor riqueza respecto a la vecina Cuba, que la hacía ser menos codiciada que esta, disminuyendo la injerencia de otras potencias en sus problemas (1969, 74).

Esta situación empezó a cambiar con la crisis económica y el aumento de la población, sumiendo la Isla en un estado de inseguridad por el aumento de la conflictividad campesina y la delincuencia. Flores señala que la comisión de delitos como robos e incendios perpetrados contra las propiedades agrícolas, riñas, embriaguez, juegos prohibidos y vagancia, entre otros, eran asociados con los sectores desposeídos, convirtiéndoles en elementos peligrosos para el mantenimiento del orden interno y para la conservación de las propiedades. El Estado y las clases propietarias sabedores que esos sectores eran los que más sufrían las consecuencias de dichas crisis, consideraron oportuno articular diversos mecanismos para ejercer sobre ellos una vigilancia constante y eficaz (1994, 240).

Por otra parte, un sector de las élites criollas empezó a mostrar su malestar con las medidas políticas y económicas tomadas por los capitanes generales, surgiendo una corriente de pensamiento liberal que propugnaba una profunda reforma económica y administrativa para la Isla. Al mismo tiempo empezó a desarrollarse un importante movimiento separatista desde el exilio. Auspiciado por los EE.UU., que había puesto

1 Entre los autores consultados que atribuyen erróneamente el proyecto del 22 de agosto de 1857 a Lemery se encuentran: Molinero, 1879, 60; Gistau, 1907, 234; Luengo, 1969, 74; Aguado, 1984, 2, 222; López, 1995, 229 y 1998, 112 y Cabo y Camino, 2003, 96.

2 Lemery hizo entrega del mando a Cotoner el 28 de enero de 1857. Nombramientos y ceses de varios gobernadores: AHN, Ultramar, 5082, Exp. 2, Docs. Nº 1 y 2.

sus intereses en la Antillas, se formó en Nueva York en 1865 la Sociedad Republicana de Cuba y Puerto Rico con sucursales en Filadelfia y Nueva Orleáns, que promovía la independencia por las armas de ambas islas.

En enero de 1868, desde su exilio en Santo Domingo, Ramón Emeterio Betances puso en marcha el Comité Revolucionario de Puerto Rico. En los meses siguientes se formaron juntas revolucionarias, consiguiendo el Comité Revolucionario financiación para la compra de armas y un transporte, *El Telégrafo*, en el que debía trasladarse Betances con un pequeño ejército a Puerto Rico una vez iniciada la revolución[3]. Señalado el levantamiento para el 29 de septiembre de 1868 en Camuy, la conspiración fue descubierta, siendo deteniendo el 20 de septiembre el líder de la junta revolucionaria de esta localidad, Manuel González. Por su parte el Gobierno dominicano a instancias del español impidió la salida de Betances y las autoridades de Saint Thomas se incautaron de *El Telégrafo* allí anclado. Para no dar tiempo a la movilización militar del Gobierno, los revolucionarios adelantaron sus planes, y el 23 de septiembre Manuel Rojas ocupó Lares proclamando la República de Puerto Rico. Las autoridades españoles sofocaron rápidamente el levantamiento, juzgando y encarcelando a los amotinados, que fueron amnistiados ese mismo año por el Gobierno tras el triunfo en la Península de la revolución que destronó a Isabel II.

Tras estos sucesos, bajo el mando de José Laureano Sanz, se estableció en la Isla un sistema militarizado de seguridad interior. El Cuerpo de Voluntarios, el Cuerpo Municipal y de Orden Público y la Guardia Civil fueron concebidos como expresión corpórea del principio de la integridad nacional y como garante de la expresión del poder de la autoridad central de la colonia. Su establecimiento facilitó la canalización de las acciones orquestadas para vigilar y contener las fuerzas que podían moverse a contrapelo de la voluntad rectora de la metrópoli y de sus representantes coloniales (Flores 1991, 217).

3. PRIMEROS PROYECTOS DE IMPLATACION DE LA GUARDIA CIVIL

Tras la creación de la Guardia Civil en la Península, el modelo de la institución fue trasladado a Cuba, organizándose en 1854 un tercio en comisión con personal voluntario del Ejército en la Isla. En Puerto Rico la organización del Cuerpo tardó más tiempo en ver la luz, al no llegar a buen puerto los proyectos planteados en 1857 y 1864, habiendo de esperar hasta 1869 para su implantación.

3.1. FERNANDO COTONER Y CHACÓN

El primer proyecto de organizar la Guardia Civil en Puerto Rico se debe al capitán general Fernando Cotoner y Chacón, conde de la Cenia, quién el 22 y 23 de agosto de 1857 elevó, respectivamente a los ministros de la Guerra y de Ultramar, la propuesta de creación de una fuerza pública inspirada en la Benemérita[4]. Esta fuerza, organizada bajo las mismas bases y reglamentos que la Guardia Civil de Cuba, debería contar

3 Las principales juntas revolucionarios fueron: "*Capa Prieto*" en Mayagüez, presidida por Mathias Bruckman, "*Centro Bravo*" en Lares, presidida por Manuel Rojas, "*Lanzador del Norte*" en Camuy, presidida por Manuel González y "*Porvenir*" en San Sebastián, presidida por Manuel Cebollero.

4 Expediente general de organización de la Guardia Civil en la isla: AHN, Ultramar, 5144, Exp. 37, Doc. 3 y Exp. 38, Doc. 25.

con dos compañías de infantería y dos de caballería de 100 hombres cada una de ellas, al mando de un comandante procedente, si era posible, de la Península (Cuadro nº 1). En base a los haberes del personal de la Guardia Civil de Cuba, su mantenimiento anual ascendería a 136.632 pesos.

	Nº de compañías	Primer Jefe 1er Comandante	Capitán Ayudante	Teniente 2º Ayudante	Sargento Brigada	Armero	Mariscal	Cabo de trompetas	Picador	Capitanes	Tenientes	Alféreces	Subtenientes	Sargentos 1º	Sargentos 2º	Cabos 1º	Cabos 2º	Furriel	Cometas	Trompetas	Guardias
P.M.	-	1	1	1	1	1	1	1	1	-	-	-	-	-	-	-	-	-	-	-	-
Infantería	2	-	-	-	-	-	-	-	-	2	2	-	4	2	6	8	8	-	4	-	172
Caballería	2	-	-	-	-	-	-	-	-	2	6	4	-	2	8	16	16	2	-	6	150
Total	4	1	1	1	1	1	1	1	1	4	8	4	4	4	14	24	24	2	4	6	322

Cuadro 1. Plantilla del Tercio de la Guardia Civil de Puerto Rico según el proyecto de Cotoner. Fuente: Elaboración propia a partir del presupuesto de creación de la Guardia Civil: AHN, Ultramar, 5144, Exp. 37, Doc. 7.

Cotoner justificaba su propuesta en el hecho de que la diseminación y aislamiento de la población isleña exigía una fuerza pública que vigilase la conducta de sus habitantes, evitando la corrupción de las costumbres, además de protegerla y ampararla de las calamidades públicas. Por otro lado, se hacía necesaria la vigilancia de las haciendas para evitar el levantamiento de los esclavos contra sus propietarios, que en más de una ocasión habían puesto en peligro la vida de sus dueños y en alarma al país. Según su opinión, la diseminación de la población y la falta de acción de las autoridades locales frustraban con frecuencia la vigilancia para la captura de desertores y criminales. Para apoyar esta afirmación Cotoner adjuntaba en su propuesta sendos informes, según los cuales 235 prófugos vagaban por la Isla, habiéndose cometido durante 1856 un total de 227 delitos de hurto, por los que fueron procesados 311 individuos.

Tras el informe emitido por el Consejo Real, por R.O. de 1 de diciembre de 1857, el proyecto fue desestimado sobre la base de que ni la índole ni el número de delitos cometidos hacía necesaria la creación de la Guardia Civil en un país de condición naturalmente dócil y sumisa, así como tampoco lo permitía el estado de la Hacienda. Para facilitar la acción de las autoridades locales, y dentro de la más estricta economía, se propuso el estudio de la creación de una Guardia Rural, basada en el carácter pacífico de los habitantes y las características topográficas de la Isla[5].

3.2. FÉLIX MARÍA MESSINA

El capitán general Félix María Messina, marqués de la Serna, retomó la idea de Cotoner, remitiendo el 30 de julio de 1864 al Ministerio de Ultramar un nuevo proyecto

5 Ibíd., Exp. 37, Doc. 8 y Exp. 38 Doc. 38.

para implantar la Guardia Civil en la Isla[6]. En el mismo se proponía la creación de una compañía de infantería y dos de caballería, con un total de 200 hombres, y los oficiales y jefes correspondientes a esta fuerza con arreglo a la organización de la Guardia Civil cubana (Cuadro nº 2).

	Nº de Compañías	Comandantes	Tenientes 1er Ayudante	Subtenientes 2º Ayudante	Capitanes	Tenientes	Subtenientes	Sargentos 1º	Sargentos 2º	Cabos 1º	Cabos 2º	Cornetas	Trompetas	Guardias
P.M.	-	1	1	1	-	-	-	-	-	-	-	-	-	-
Infantería	1	-	-	-	1	1	2	1	2	3	-	2	-	80
Caballería	2	-	-	-	2	2	2	2	2	4	6	-	4	120
Total	-	1	1	1	3	3	4	3	4	7	6	2	4	200

Cuadro 2º. Plantilla del Tercio de la Guardia Civil de Puerto Rico según el proyecto de Messina. Fuente: Elaboración propia a partir del presupuesto de creación de la Guardia Civil: AHN, Ultramar, 5144, Exp. 38, Doc. 3 y 4.

El principal objeto de esta fuerza sería evitar la desafección al trabajo y la falta de ocupación de la población que vagaba por las zonas rurales. Para ello debía vigilarse constantemente la red de caminos carreteros y vecinales de importancia, cuya extensión se calculaba en 300 leguas, estableciéndose puesto de cuatro hombres cada seis leguas (Cuadro nº 3). Messina consideraba que la Guardia Civil podía desarrollar con ventaja y eficacia los servicios desempeñados por los guardias municipales, urbanos y rurales, al contar con un prestigio y una fuerza moral del que carecían estas policías.

	Leguas	**Nº de guardias**
Capital	54	36
Caguas	42	28
Humacao	20	13
Guayama	18	12
Ponce	56	37
San Germán	10	7
Mayagüez	20	14
Aguadilla	36	24
Arecibo	44	29
	300	200

Cuadro 3º. Número de leguas de cada distrito y fuerza que debía asignarse a cada uno de ellos. Fuente: AHN, Ultramar, 5144, Exp. 38, Doc. 5.

El mantenimiento de la Guardia Civil debía ser financiado por los municipios y por la Hacienda Pública, calculándose su coste mensual en 102.527 pesos. Los municipios

6 Ibíd., Exp. 38, Doc. 2.

contribuirían con 59.100 pesos, que saldrían de la partida asignada al mantenimiento de la guardia municipal, urbana y rural, siendo aportada la cantidad restante por el Estado.

Por R. O. de 12 de noviembre de 1866, a la vista de los informes emitidos por las Secciones de Ultramar y Guerra y Marina, el expediente fue desestimado[7]. Nuevamente se consideraba que el carácter dócil y pacífico de la población hacía innecesaria la Guardia Civil al contar ya con la Guardia Rural, a lo que se unía el precario estado de la Hacienda Pública.

4. IMPLANTACIÓN DE LA GUARDIA CIVIL DE PUERTO RICO

Tras el Grito de Lares de 1868, eran cada vez más las voces que pedían que se organizara la Guardia Civil en la Isla. La presión de los hacendados y el temor de que el movimiento insurreccional en que se encontraba Cuba se trasladara a Puerto Rico, puso en marcha los mecanismos para la organización de un tercio de la Guardia Civil.

4.1. CREACIÓN DE UN TERCIO PROVISIONAL

El 10 de enero de 1869, el capitán general José Laureano Sanz y Posse solicitó al ministro de la Guerra la creación de un tercio de la Guardia Civil, al considerar que este Cuerpo era el único elemento capaz de robustecer el principio de autoridad en todos los puntos de la Isla. El tercio estaría compuesto por 200 hombres de infantería y 50 de caballería, organizados en dos compañías mixtas[8]. El ministro de la Guerra remitió a su homólogo de Ultramar la comunicación del capitán general, junto a los antecedentes existentes sobre el asunto, para que resolviera con la premura que el caso requería.

Igualmente, Sanz solicitó al ministro de Ultramar el urgente despacho del asunto, argumentando que tenía muy avanzados los trabajos preparatorios para la organización de la Guardia Civil y que los pueblos demandaban la implantación de la Institución, contribuyendo con donativos para sufragar parte de los gastos. Además, manifestaba que la implantación de la Guardia Civil contribuiría al afianzamiento del orden público y a reanimar entre los habitantes de la Isla su adhesión a la causa de la nacionalidad española[9].

Desde la Capitanía General se solicitó, a los jefes de los batallones de guarnición en la Isla, la relación del personal que deseara ingresar en la Guardia Civil y que reunieran los siguientes requisitos:

- Que supieran leer y escribir.
- Intachable conducta.
- Robustez.
- Que no bajaran de cinco pies y una pulgada de estatura.

7 Ibíd., Exp. 38, Doc. 16.
8 Expediente sobre la Organización de la Guardia Civil de Puerto Rico: AHMM, Sig. 5205.1 e Ibíd., Exp. 38, Doc. 23.
9 Ibíd., Exp. 38, Doc. 29.

- Buena presencia.
- Que les faltase por lo menos cuatro años de servicio o se reengancharan sin premio el completo de ese plazo y que hubiesen terminado la instrucción de recluta.

Figurando en relación separada los que no llevasen un año de servicio[10].

El 10 de abril fueron remitidos al Ministerio de Ultramar los reglamentos para el servicio y militar para su aprobación, dándose cuenta a la vez de haberse adelantado la instalación provisional de la Guardia Civil por razones de orden público. Para ello se había sacando el personal necesario del Ejército, sufragando los gastos con los donativos recibidos de los hacendados y los pueblos para no ocasionar perjuicio al erario público, solicitando Sanz la aprobación de todo lo actuado hasta ese momento[11]. Una semana después comunicaba las disposiciones tomadas para la compra de 50 caballos y del vestuario del personal, volviendo a insistir en la urgente necesidad de tomar una resolución definitiva sobre el asunto "en bien del servicio y de la causa del orden público y de integridad nacional"[12].

En el mes de mayo se dieron las instrucciones para la formación de la 1ª compañía del Tercio de la Guardia Civil con el personal seleccionado de los batallones de Artillería, Madrid y Puerto Rico. Este personal quedó instalado en el cuartel de Ballajá a las órdenes del comandante graduado, capitán Vicente Larroche Sierra, jefe de la compañía, y del teniente Juan Babiano, para la instrucción teórica en la Cartilla de la Guardia Civil y demás disposiciones referentes al Instituto. Igualmente se dispuso que por el Cuerpo de Artillería se hiciese entrega de 100 fusiles *Remingthon* y 1.000 cápsulas y por el 1er Regimiento de Caballería de 34 monturas completas e igual número de sables[13].

El 13 de junio de 1869, el Poder Ejecutivo aprobó interinamente todo lo actuado hasta el momento por Sanz sobre el establecimiento de la Guardia Civil en la Isla.

Al gobernador superior civil de la isla de Puerto Rico

Madrid 13 de junio de 1869

E. S. Vistas las cartas, números 111, 124, 125 y 136 de 13 de marzo, 10 y 17 de abril último sobre el establecimiento de la Guardia Civil en esa provincia y los reglamentos para su organización y servicio, el Poder Ejecutivo, en el ejercicio de sus funciones y de conformidad con lo propuesto por las Secciones de Ultramar y de Guerra y Marina del Consejo de Estado, ha resuelto aprobar lo hecho por V. E. y dispone que se le devuelvan los citados reglamentos, como se verifica, a fin de que sobre ellos informe el Consejo de Administración de la Isla; y por último que se prevenga a V. E. se mantenga la interinidad que ha creado, mientras se evacuan dichos informes y pueda dictarse por el Gobierno la aprobación definitiva del Instituto de que se trata. Lo digo a V. E. d. o. …

4.2. DESPLIEGUE Y ORGANIZACIÓN DEL TERCIO

El 19 de julio de 1869 se dispuso que la 1ª compañía saliera a prestar servicio al mando del capitán Larroche, procediéndose a la distribución de la fuerza de acuerdo

10 Ibíd., Sig. 5205.1.
11 Ibíd., Exp. 39, Doc. 2.
12 Ibíd., Exp. 39, doc. 25.
13 Ibíd., Sig. 5205.1. El reglamento provisional para el servicio se puede consultar en la Gaceta de Puerto Rico, Nº 86.

a las necesidades expresadas por los comandantes militares y corregidores. La compañía constaba de tres secciones de infantería y una sección de caballería. Cada sección de infantería se dividía en tres brigadas de 10 hombres cada una de ellas y la de caballería de tres brigadas de 11 hombres. La fuerza quedó distribuida el 12 de agosto de la siguiente manera[14]:

- Departamento de Mayagüez: Tres brigadas de infantería y una de caballería. Puestos: Guanica, Pedernales, Sabana Grande, Hormigueros, El Maricao, Hatillo de Mayagüez y Lajas (con cuatro hombres cada uno de ellos), Mayagüez (cinco hombres) y Las Marías (seis hombres).
- Departamento de Aguadilla: Dos brigadas de infantería. Puestos: Resicora, San Sebastián, Lares e Isabela (con cuatro hombres cada uno de ellos) y Moca (cinco hombres).
- Departamento de Arecibo. Tres brigadas de infantería y uno de caballería. Puestos: Quebradillas, Hatillo, Pajuil, Palomar, Arecibo en Q., Utuado, Ciales, Manatí (Con cuatro hombres cada uno de ellos) y Arecibo (con seis hombres).
- En la Capital quedó en depósito hasta nueva orden una brigada de infantería y otra de caballería que debía ser destinada al departamento de Bayamón.

El 2 de agosto se dio orden que el personal seleccionado para formar la 2ª compañía se acuartelara en Ballajá, a las órdenes del capitán de Infantería José Tous y Coll, para comenzar la instrucción.

Para poner en marcha la organización del Tercio recién creado se comisionó al comandante del Batallón de Cádiz, Bernardino Quintes y Solares, pasando su primera revista administrativa en el mes de octubre. El personal, que hasta ese momento se encontraba en comisión percibiendo sus haberes de soldado más un plus de seis reales de vellón, pasó a percibir los mismos haberes que la Guardia Civil de Cuba.

El 22 de octubre de 1869, formada ya la 2ª compañía, se ordenó al capitán Tous procediera a distribuir la fuerza, desplegándose en los departamentos de Huamaco, Bayamón, Guayama y Ponce, estableciéndose la cabecera de la compañía en Caguas.

Para el mando del Tercio fue designado el teniente coronel Jerónimo de la Torre y Velasco, siendo alta en la revista del mes de noviembre, ocupando el cargo de 2º jefe el comandante Quintes. La fuerza orgánica de Tercio quedó formada por dos jefes, 11 oficiales y 254 clases de tropas (Cuadro Nº 4).

14 Ibíd. Sig. 5205.1.

	Jefes y Oficiales					Tropa Infantería								Tropa de Caballería							Total		
	Teniente Coronel	Comandante	Capitanes	Tenientes	Alféreces	Sargento 1º	Sargento 2º	Cabos 1º	Cabos 2º	Cornetas	Guardia 1º	Guardia 2º	Total	Sargento 2º	Cabos 1º	Cabos 2º	Trompetas	Guardia 1º	Guardia 2º	Total	Jefes	Oficiales	Tropa
Plana Mayor	1	1	-	1	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	2	1	-
1ª Compañía	-	-	1	2	2	1	2	3	3	3	36	45	93	1	1	1	1	15	15	34	-	5	127
2ª Compañía	-	-	1	2	2	1	2	3	3	3	36	45	93	1	1	1	1	15	15	34	-	5	127
Total	1	1	2	5	4	2	4	6	6	6	72	90	186	2	2	2	2	30	30	68	2	11	254

Cuadro 4º. Plantilla del Tercio de la Guardia Civil de Puerto. Fuente: Elaboración propia a partir del proyecto de Reglamento Militar.

Por orden de 11 de noviembre de 1869 fueron aprobados los reglamentos para el servicio y militar con carácter de interinidad, hasta que no se aprobara la nueva organización administrativa de Puerto Rico que se estaba tramitando en las Cortes[15].

La práctica sobre el terreno puso en evidencia lo penoso que resultaba el servicio para la infantería, debido al clima y a las características orográficas de la Isla, que dificultaban el tránsito de los caminos y el vadeo de los ríos en época de lluvia o avenidas. A la vista de estas circunstancias, por orden de 12 de enero de 1870, se aprobó un aumento de 46 hombres en las secciones de caballería, para crear parejas mixtas, siendo alta en la revista del mes de abril[16]. Habiéndose llevado a efecto la instrucción y organización de la misma en Río Piedras, a las órdenes de los tenientes José Jiménez y Domingo Sánchez, la fuerza fue distribuida en los departamentos de Bayamón, Huamaco y Guayama.

El 25 de junio el teniente coronel Jerónimo de la Torre fue nombrado comandante militar de Arecibo, suprimiéndose por R.O. de 8 de agosto de 1870 la plaza de teniente coronel del Tercio, siendo destinado como 1er jefe al comandante Antonio de la Huerta y González[17].

5. AMALGAMA DE 1871 Y CONSOLIDACIÓN DEL TERCIO

La Guardia Civil de Puerto Rico, organizada para prestar el servicio del Instituto con el carácter de interinidad, tuvo su consolidación con el proceso de amalgama iniciado en 1871 para unificar los Tercios de Ultramar con los de la Península. Para llevar a cabo esta reforma el Gobierno se fundó en los favorables resultados obtenidos por el Tercio desde su creación y en la necesidad que existía de hacer extensiva a la Isla las garantías que exigía la índole especial del Instituto, así como imbuir en su personal el espíritu de Cuerpo de que se carecía, por pertenecer a él en comisión y sin los derechos que su reglamento concedía[18].

15 Ibíd., Exp. 39, Doc. 23. El articulado completo de los reglamentos se puede consultar en la Gaceta de Puerto Rico, Nº 5, 1870.

16 Ibíd. Sig. 5205.1.

17 Memorias de actividades de la Guardia Civil en Puerto Rico en los años 1870-1873: AHMM., Sig. 5205.2.

18 RR.OO. de 10 de julio de 1871 y 6 de febrero de 1872. Para la amalgama ver Luengo, 1970, 120-126; Aguado, 1984, 3, 9-12 y López, 1995, 231-237 y 1998, 113-120.

Por R.O. de 11 de junio de 1872 se declaró unificado el Tercio de Puerto Rico a los demás del Cuerpo, pasando a regirse para su servicio peculiar por lo dispuesto en la Cartilla de la Guardia Civil y demás disposiciones sobre el mismo. Igualmente, se concedió el ingreso en las escalas del Cuerpo a los jefes y oficiales que lo solicitaron, quedando el resto agregados hasta su baja por ascenso u otra circunstancia[19].

El 23 de octubre de 1872 se aprobó el Reglamento Militar para la Guardia Civil de Ultramar, adaptándolo a las peculiaridades de las colonias. Las principales diferencias con el reglamento de la Península eran:

- El capitán general de Puerto Rico era su director nato, creándose la figura del subdirector general, para apoyar a este en sus funciones.
- La Guardia Civil dependía del capitán general en todo lo concerniente a su organización, personal, disciplina, material y percibo de haberes, y del gobernador superior civil en cuanto a su servicio especial y acuartelamiento.
- El personal reclutado procedería: 1º) del personal de los Cuerpos e Institutos del Ejército de Puerto Rico con más de un año se servicio, 2º) de los licenciados del Ejército de la Isla y 3º) de los Cuerpos de la Península o licenciados del mismo.

Para el cargo de subinspector fue destinado el teniente coronel del 9º Tercio, José Castrillón Polledo, que propuso la reorganización del Tercio para adecuarla a lo prevenido en el Reglamento Militar. La nueva organización fue aprobada por R.O. de 25 de agosto de 1873, suprimiéndose el carácter mixto de las compañías, creándose dos compañías de infantería y un escuadrón de caballería, que formaron una comandancia de 1º clase, al mando del teniente coronel Miguel Galiano Enriques, procedente del 5º Tercio[20]. El número de puestos se redujo de 67 a 46, para que fueran mandados por oficiales, sargentos y cabos, suprimiéndose en la plantilla 15 plazas de guardia 1º y aumentándose en cuatro oficiales, tres sargentos y 12 cabos[21].

Por orden de 29 de septiembre de 1874 la plantilla se incrementó hasta los 500 efectivos con dos tenientes, dos alféreces y 100 de clases de tropa en la infantería y con igual número de efectivos más un capitán en la caballería, formándose un segundo escuadrón[22].

6. REORGANIZACIONES Y AUMENTOS DE LA FUERZA

6.1. ORGANIZACIÓN DEL TERCIO EN DOS COMANDANCIAS (1876)

La diseminación de los puestos, la falta de comunicaciones y la orografía del terreno, que dificultaba las revistas y la acción del mando, puso de manifiesto la necesidad de llevar a cabo una reorganización del Tercio para una mayor eficacia en el servicio. Por R.O. de 2 de junio de 1876 el Tercio se organizó en dos comandancias, creándose una tercera compañía de infantería, contado cada una de ellas, al igual que los

19 Informe sobre la situación de la Guardia Civil en Puerto Rico: AHMM, Sig. 5205.7.
20 Ibíd., Sig. 5205.2.
21 Reorganización de la Guardia Civil en Puerto Rico: AHMM, Sig. 5205.9.
22 Ibíd., 5144, Exp. 34, Doc. 28.

dos escuadrones de caballería, con 100 hombres[23]. El Tercio quedó organizado de la siguiente manera:

- Plana Mayor.
- Comandancia de Puerto Rico de 1ª clase, al mando de un teniente coronel y un comandante segundo jefe: 1ª y 2ª compañía de infantería y 1er escuadrón de caballería.
- Comandancia de Ponce de 2ª clase, al mando de un comandante y un capitán segundo jefe: 3ª compañía y 2º escuadrón de caballería.

6.2. REDUCCIÓN DE LA PLANTILLA (1885)

En los presupuestos del ejercicio económico 1885-1886 se redujo la partida destinada al capítulo de personal, reduciéndose la plantilla en la revista del mes de agosto de 1885 en 52 hombres la infantería y en 25 la caballería, pasando a contar con 423 efectivos. Para llevar a cabo esta disminución se dispuso que no se cubrieran las vacantes que se fueran produciendo hasta llevarse a cabo el reajuste de la plantilla[24].

6.3. SUPRESIÓN DE LA SUBDIRECCIÓN (1886)

Por R.O. de 12 de septiembre de 1886 se suprimió la subdirección, reunificándose las dos comandancias en una sola al mando de un teniente coronel y un comandante 2º jefe encargado del detall. La plantilla se disminuyó en un coronel subdirector, un comandante y dos capitanes, que pasaron a la Península, aumentándose en 27 guardias 2º de infantería. La nueva comandancia pasó su primera revista de comisario en el mes de noviembre, al mando accidental del comandante Juan Herrera y Rubín de Celis[25].

6.4. REORGANIZACIÓN DE 1888

Por R.O. de 21 de septiembre de 1888 se dispuso el restablecimiento de la plaza de coronel subdirector, siendo nombrado para el cargo al coronel Benito Macías y Rueda, dividiéndose la comandancia en dos, con cabeceras en Puerto Rico y Ponce. Por R.O. de 8 de marzo de 1889 se aprobó el aumento en la plantilla en un comandante y un capitán para organizar la plana mayor de la comandancia de Ponce[26]. Esta reforma, sin embargo, no fue consignada en la ley de presupuestos para el ejercicio económico de 1889-1890, por lo que el capitán general dejó sin efecto la misma suprimiendo la plaza de coronel subinspector, quedando la organización del Tercio conforme se había establecido en 1886[27].

23 Reorganización de la Guardia Civil en Puerto Rico: AHMM, Sig. 5605.13.

24 Aumento de la plantilla de la Guardia Civil en Puerto Rico: AHMM, Sig. 5605.03.

25 Reorganización de la Guardia Civil en Puerto Rico: AHMM, Sig. 5205.17 y Organización de una 3ª Compañía de la Guardia Civil y supresión de las Milicias de Puerto Rico: AHMM. Sig. 5605.5.

26 Restablecimiento de la plaza de coronel subinspector y organización de la Guardia Civil de Puerto Rico en dos Comandancias: AHM, Sig. 5205.36. Por R.O. de 18 de diciembre se destinan para cubrir las plazas aumentadas al capitán Ramón Arsaez Ferrando y al comandante Antonio Carrera Vircarri. DOME Nº 280.

27 Ibíd, Sig. 5205.36 e Ibíd., 5144, Exp. 41, Doc. 4.

6.5. AUMENTO DE LA FUERZA DE INFANTERÍA (1890)

Por R.O. de 24 de diciembre de 1890, atendiendo al aumento de la criminalidad, a las condiciones topográficas de la Isla y la escasa fuerza existente, la plantilla se incrementó en 20 cabos, 20 guardias 1º y 160 guardias 2º, alcanzando los 654 efectivos[28].

El reemplazo de las vacantes resultaba difícil ante la falta de personal en la Isla que reuniera los requisitos para su ingreso en el Cuerpo. Esta dificultad se vio agravada al extenderse a Puerto Rico la orden de que el personal casado o viudo con hijos a su cargo no fuesen destinados de la Península a la Isla de Cuba. Para llevar a cabo este aumento de plantilla, desde la capitanía general se instó a los jefes de las unidades del Ejército a fomentar entre el personal a su mando el pase a la Guardia Civil. Para facilitar el ingreso el plazo mínimo de servicio quedó reducido al necesario para haber adquirido y completado la instrucción reglamentaria. Al no haber suficientes voluntarios con la estatura mínima exigida, esta fue reducida para facilitar su pase al Cuerpo.

6.6. CREACIÓN DE LA 4ª COMPAÑÍA (1894)

Con el aumento llevado en la fuerza de infantería se establecieron 27 puestos nuevos, llegando su número a los 100, creciendo la extensión de la demarcación de las compañías. Esta circunstancia, unida a la orografía y a la dificultad en las comunicaciones en época de lluvia, impedía la acción inspectora de los capitanes de compañía, quedando sus visitas a los puestos más alejados, reducidas a las revistas mensuales. Para facilitar esta labor de inspección por R.D. de 31 de mayo de 1894 se reorganizó la fuerza de infantería creándose una cuarta compañía[29].

6.7. ORGANIZACIÓN DE UN NUEVO TERCIO (1897)

En 1897 Puerto Rico fue dividido en dos regiones con un delegado al frente de cada una ellas, con las mismas atribuciones en lo referente al orden público que los gobernadores civiles en la Península. Para adaptar la organización de la Guardia Civil a la administrativa de la Isla, por R.O. de 12 de julio de 1897 se crea el Tercio de Puerto Rico, estableciéndose una comandancia en cada región. El Tercio quedó al mando del coronel Eusebio Pacheco Llaurado, la comandancia de Puerto Rico de primera clase, con la 1ª, 2ª compañía y 1er escuadrón, al mando del teniente coronel Pedro Pérez Miquelini y la de Ponce de 2ª clase, con la 3ª, 4ª compañía y 2º escuadrón, al mando del comandante Julián Alonso Ariza[30].

6.8. PROPUESTA DE REAGRUPACIÓN DE PUESTOS (1898)

En 1898 la fuerza del Tercio se encontraba diseminada en 110 puestos formados por 4 o 5 hombres, que en caso de alteración del orden público o tenerse que defender de una agresión no podrían hacerlo adecuadamente. Además, algunos de estos puestos se encontraban establecidos en despoblados y en zonas de escasa importancia,

28 Reorganización de la Guardia Civil en Puerto Rico: AHMM, Sig. 5205.23.

29 Propuesta de creación de una nueva Compañía de la Guardia Civil en Puerto Rico: AHMM, Sig. 5205.24 y Organización de la Guardia Civil de Puerto Rico entre los años 1888 y 1894: AHMM, Sig. 5605.6.

30 Creación de una segunda Comandancia de la Guardia Civil en Puerto Rico: AHMM, Sig. 5205.26.

sin las infraestructuras básicas para la vida de los guardias y sus familias. Por todo ello el 28 de febrero de 1898, el subinspector del Tercio elevó al capitán general una propuesta para la supresión de 31 puestos, distribuyendo la fuerza entre el resto para que su dotación estuviera formada por entre ocho y 12 hombres. El 30 de marzo, el proyecto fue devuelto a la Subinspección para el reajuste de las plantillas de algunos puestos antes de proceder a su aprobación[31].

Dado el estado de guerra con EE.UU. se desconoce si este proyecto llegó a ponerse en práctica. El 12 de mayo de 1898 la escuadra estadounidense, al mando del almirante Sampson, bombardeaba San Juan, comenzando el bloqueo de Puerto Rico. El 25 de julio las tropas estadounidenses desembarcaban en Guánica y Yauco, dando comienzo las operaciones terrestres. La Guardia Civil se concentró participando en la defensa de la Isla, tomando parte en las acciones de Coamo, Asomonte, Guayama, Guasio y faro Fajardo, teniendo un muerto, tres heridos y un contuso.

El 12 de agosto se firmó el armisticio que puso fin a la guerra Hispanoamericana y por el que España cedía a EE.UU. las colonias de Ultramar. Durante el mes de octubre se llevó acabo la evacuación de Puerto Rico, siendo el personal del Tercio repatriado a España[32].

7. CONCLUSIÓN

El tema de la presencia de la Guardia Civil en Puerto Rico ha pasado casi desapercibido para los autores que han tratado la historia del Cuerpo, quedando sus referencias siempre vinculadas a lo que sucedía en la vecina Cuba. Casi todos los autores se han limitado a reproducir lo expuesto por Molinero y Gistau, esto ha llevado, junto a la escasa información aportada sobre el tema, a que todos ellos hayan cometido el error de atribuir el primer proyecto de creación de la Guardia Civil en Puerto Rico a José Lemery.

En el presente trabajo, a la vista de la información aportada por las fuentes de archivo, se ha rectificado esta autoría atribuyéndosela a su verdadero artífice: el capitán general Fernando Cotoner y Chacón. Con la exposición de los proyectos de la implantación de la Guardia Civil en Puerto Rico, su proceso de creación y posteriores reorganizaciones, se ha querido dar un primer paso que de pie para un estudio más amplio sobre la presencia del Cuerpo en la Isla. Así, por ejemplo, debería analizarse entre otros temas la labor desarrollada por la Guardia Civil en la desarticulación del movimiento secesionista o llevar a cabo una recopilación de los servicios realizados en la isla. Sirva pues este artículo para dar a conocer un poco más la presencia de la Guardia Civil en las antiguas colonias españolas de Ultramar.

31 Reorganización de los Puestos de la Guardia Civil en Puerto Rico: AHMM. Sig. 5176.1.

32 El personal del Tercio fue repatriado en los vapores *Isla de Panay*, *Patricio Satrústegui*, *Reina María Cristina*, *Covadonga*, *Gran Antilla* y *Montevideo* y el personal enfermo que se encontraba en el hospital de Puerto Rico lo fue en el vapor *Alicante*. Las relaciones de los repatriados de Ultramar aparecen publicadas en Guardia Civil. Resumen de servicios, disposiciones y asuntos de peculiar para el Instituto de 1899 y 1900. (Esta publicación sustituyó al Boletín Oficial del Cuerpo entre 1889 y 1907).

PLANTILLA REGLAMENTARIA DE LA GUARDIA CIVIL DE PUERTO RICO A 1 DE ENERO																															
	PM DEL TERCIO						PM COMD.				JEFES Y OFICIALES				TROPA										TOTALES						
Año	Coronel Subinspector	Tte. Coronel	Comandantes	Capitán Ayudante	Tte. ayudante / Habilitado	Maestro armero	Teniente Coronel	Comandantes	Capitán 2º Jefe / Ayudante	Maestro armero	Capitán	Teniente / 1ª Teniente	Alférez / 2º Teniente	Veterinarios	Sargento 1º	Sargento 2º	Corneta	Trompeta	Cabo 1º	Cabo 2º	Guardia 1º	Guardia 2º	Herrador	Forjador	Jefes	Oficiales	Tropa	Tropa Infantería	Tropa Caballería	Caballos jefes y oficiales	Caballos tropa
1869*	-	1	1	-	1	-	-	-	-	-	2	4	4	-	2	6	6	2	8	8	102	120	-	-	2	11	254	186	68	13	68
1870	-	1	1	-	1	-	-	-	-	-	2	4	4	-	2	6	6	2	8	8	102	120	-	-	2	11	254	186	68	13	68
1871	-	-	1	1	1	-	-	-	-	-	2	4	4	-	2	8	6	2	12	12	102	150	4	2	1	12	300	186	114	14	114
1872	-	-	1	1	1	-	-	-	-	-	2	4	4	-	2	8	6	2	12	12	102	150	4	2	1	12	300	186	114	14	114
1873	1	-	1	1	1	-	-	-	-	-	2	4	4	-	2	8	6	2	12	12	102	150	4	2	2	12	300	186	114	14	114
1874	1	1	1	-	1	-	-	-	-	-	3	6	6	-	3	10	5	2	18	18	87	151	6	-	3	16	300	186	114	14	114
1875	1	1	1	-	1	-	-	-	-	-	4	10	10	-	4	16	6	4	28	28	102	300	12	-	3	25	500	286	214	-	214
1876	1	1	1	1	-	-	-	-	-	-	4	10	10	-	4	16	6	4	28	28	102	300	12	-	3	25	500	286	214	-	198
1877	1	-	-	1	-	-	1	2	1	-	5	10	10	-	5	15	6	4	25	25	100	320	-	-	4	27	500	300	200	-	174
1878	1	-	-	1	-	-	1	2	1	-	5	10	10	-	5	15	6	4	25	25	100	320	-	-	4	27	500	300	200	-	174
1879	1	-	-	1	-	-	1	2	1	-	5	10	10	2	5	15	6	4	25	25	100	320	-	-	4	27	500	300	200	-	174
1880	1	-	-	1	-	1	-	2	2	-	5	10	10	2	5	15	6	4	25	25	100	320	-	-	3	28	500	300	200	-	174
1881	1	-	-	1	-	1	-	2	2	-	5	10	10	2	5	15	6	4	25	25	100	320	-	-	3	28	500	300	200	-	174
1882	1	-	-	1	-	1	-	2	2	-	5	10	10	2	5	15	6	4	25	25	100	320	-	-	3	28	500	300	200	-	174
1883	1	-	-	1	-	1	-	2	2	-	5	10	10	2	5	15	6	4	25	25	100	320	-	-	3	28	500	300	200	-	174
1884	1	-	-	1	-	1	-	2	2	-	5	10	10	2	5	15	6	4	25	25	100	320	-	-	3	28	500	300	200	-	174
1885	1	-	-	1	-	1	-	2	2	-	5	10	10	2	5	15	6	4	25	25	100	320	-	-	3	28	500	300	200	-	174
1886	1	-	-	1	-	1	-	2	2	-	5	10	10	2	5	13	6	4	23	23	96	253	-	-	3	28	423	248	175	-	149
1887	-	-	-	-	-	-	1	1	1	1	5	10	10	2	5	13	6	4	23	23	96	280	-	-	2	26	450	275	175	-	149
1888	-	-	-	-	-	-	1	1	1	1	5	10	10	2	5	15	6	4	25	25	40	334	-	-	2	26	454	276	178	-	149
1889	1	-	-	1	-	1	1	2	1	-	5	10	10	2	5	15	6	4	25	25	40	334	-	-	2	26	454	276	178	-	149
1890	-	-	-	-	-	-	1	1	1	1	5	10	10	2	5	15	6	4	25	25	40	334	-	-	3	27	454	276	178	-	149
1891	-	-	-	-	-	-	1	1	1	1	5	10	10	2	20		6	4	70		60	494	-	-	2	26	654	476	178	-	149
1892	-	-	-	-	-	-	1	1	1	1	5	10	10	2	20		6	4	70		60	494	-	-	2	26	654	476	178	-	149
1893	-	-	-	-	-	-	1	1	1	1	5	10	10	2	20		6	4	70		60	494	-	-	2	26	654	476	178	-	149
1894	-	-	-	-	-	-	1	1	1	1	5	10	10	2	20		6	4	70		60	494	-	-	2	26	654	476	178	-	149
1895	-	-	-	-	-	-	1	1	1	1	6	12	8	2	20		8	4	70		60	492	-	-	2	29	654	476	178	31	149
1896	-	-	-	-	-	-	1	1	1	1	6	12	8	2	20		8	4	70		60	492	-	-	2	29	654	476	178	31	149
1897	-	-	-	-	-	-	1	1	1	1	6	12	8	2	22		8	4	71		64	577	-	-	2	29	746	476	270	31	250
1898	1	-	-	1	-	1	1	2	1	1	6	12	8	2	22		8	4	71		64	577	-	-	4	30	746	476	270	33	250
* Primera plantilla establecida en el Reglamento Militar aprobado provisionalmente el 11 de noviembre de 1969.																															

Cuadro Nº 5. Plantilla reglamentaria del Tercio de Puerto Rico a 1 de enero de cada año. Fuente Elaboración propia.

ARCHIVOS CONSULTADOS

Archivo Histórico Nacional. Sección de Ultramar.

Archivo Histórico Militar de Madrid. Capitanía General de Puerto Rico.

BIBLIOGRAFÍA CITADA

Aguado Sánchez, F. (1985). *Historia de la Guardia Civil*. Madrid: Planeta.

Camino del Olmo, M. A. y Cabo Meseguer, V. (2003). *La Policia Española de Ultramar. Cuba y Puerto Rico*. Madrid: Almena Ediciones.

Flores Collazo, M. M. (1994). “Expansión del poder estatal y la militarización del sistema de orden público en el Puerto Rico del Siglo 19”, en *OP. CIT. Boletín del Centro de*

Investigaciones Históricas, 8, 203-246.

Gistau Ferrando, M. (1907). *La Guardia Civil. Historia de esta Institución*. Valdemoro: Imprenta de la Guardia Civil.

López Corral, M. (1995). *La Guardia Civil. Nacimiento y consolidación 1844-1874*. Madrid: Secretaria Técnica, Ministerio del Interior.

López Corral, M (1998). "La Guardia Civil en Ultramar", en López Valdivieso, Santiago (coord.), *La Guardia Civil de 1898*. Madrid: Dirección General de la Guardia Civil, 107-136.

Luengo Muñoz, M. (1969). "La Guardia Civil en la Isla de Cuba y Puerto Rico (I)", en *Revista de Estudios Históricos de la Guardia Civil*, 5, 109-136.

Luengo Muños, M. (1970). "La Guardia Civil en la Isla de Cuba y Puerto Rico (II)", en *Revista de Estudios Históricos de la Guardia Civil*, 6, 23-36.

Molinero y Gómez-Cornejo, Andrés (1879). *Compilación de las disposiciones referentes a la Guardia Civil de Puerto Rico.* Puerto Rico: Establecimiento Tip. del Boletín.

Fecha de recepción: 28/10/2016. Fecha de aceptación: 20/12/2016

EL USO DE LAS NUEVAS TECNOLOGÍAS POR EL TERRORISMO YIHADISTA

RODRIGO LODEIRO CORRAL

COMANDANTE DE LA GUARDIA CIVIL. SECCIÓN DE OPERACIONES DEL ESTADO MAYOR DE MANDO DE OPERACIONES DE LA GUARDIA CIVIL

RESUMEN

Partiendo de las diferentes publicaciones oficiales que existen sobre esta materia, especialmente el documento “El uso de Internet con fines terroristas” de la Oficina de las Naciones Unidas contra la Droga y el Delito, este artículo tiene como finalidad el análisis de los actuales instrumentos que, principalmente desde el punto de vista judicial, técnico y policial, existen. Y, por otro lado, fruto de las entrevistas mantenidas con expertos de la lucha antiterrorista y la experiencia del autor en esta materia, proponer cuáles serían los instrumentos idóneos y cuál sería el camino a seguir para invertir el imparable aumento en la utilización de las nuevas tecnologías, por parte de las organizaciones terroristas de carácter yihadista, para cometer atentados o acciones terroristas.

Hay circunstancias que convierten a España en objetivo del terrorismo internacional: la vecindad con regiones inestables como el Sahel, la posible y creciente radicalización de los emigrantes tanto de primera como de segunda generación, las reivindicaciones del islamismo radical sobre este país como parte del imaginario del Islam, y su determinante implicación en la lucha contraterrorista.

El uso de las nuevas tecnologías, con la finalidad última de cometer una acción terrorista al uso o en la modalidad de ciberataque, es un problema transnacional que exige una acción coordinada e integrada entre los diferentes estados del sistema interestatal.

Sin embargo, a la ausencia de una gobernanza global de Internet, se suma otra gran dificultad a la hora de establecer una estrategia global contra este fenómeno, que es la necesidad de conocimientos técnicos para la investigación eficaz de estos delitos, así como la homologación de los procedimientos utilizados para obtención de información y garantizar su validez para sostener la imputación en el posterior proceso penal.

Por otro lado, una estrategia eficaz contra el terrorismo a través de las nuevas tecnologías exige una cooperación policial ágil e implicación de todos los actores competentes en el asunto: Estados miembros de las principales Organizaciones Internacionales, servicios policiales, de inteligencia, del ámbito de la ciberdefensa jueces y compañías proveedoras de servicios de tecnologías de la información.

Palabras clave: ciberyihad, nuevas tecnologías, redes sociales, mensajería instantánea, reclutamiento¸ radicalización, incitación al terrorismo, financiación, adiestramiento y planificación.

ABSTRACT

On the basis of the various official publications on this subject, in particular the document “Internet use for terrorist purposes” of the United Nations Office on Drugs and Crime, this article has the purpose of analyzing the currently existing instruments, mainly from the judicial, technical and police point of view. On the other hand, as a result of interviews with experts on the fight against terrorism and the author’s experience in this area, this article proposes what the ideal instruments would be and what the way to continue to reverse the unstoppable increase in the use of new Technologies, would be by terrorist organizations of a jihadist nature, to commit terrorist attacks or actions.

There are circumstances that make Spain the target of international terrorism: the proximity to unstable regions such as the Sahel, the possible and growing radicalization of both first and second generation immigrants, radical Islamist claims on this country as part of Imaginary of Islam, and its decisive implication in the fight against terrorism.

The use of new technologies, with the ultimate aim of committing a traditional terrorist action or in the cyberattack mode, is a transnational problem that requires a coordinated and integrated action between different states.

However, added to the absence of global internet governance, there is another great difficulty in establishing a comprehensive strategy against this phenomenon, which is the need for technical knowledge for the effective investigation of these crimes, as well as the homologation of Procedures used to obtain information and the guarantee of its validity to support the charging in the subsequent criminal proceedings.

On the other hand, an effective counter-terrorism strategy through the use of new technologies requires police cooperation and the involvement of all relevant actors in the matter, Member States of the main International Organizations, police services, intelligence services, Cyberdefense, judges and companies providing information on technology services.

Keywords: ciberjihad, new technologies, social networks, instant messaging, recruitment, radicalization, incitement to terrorism, financing, training and planning.

1. INTRODUCCIÓN

Cuando en el año 2002 Osama Bin Laden, en una carta dirigida al Mullah Omar en Afganistán, afirmaba lo siguiente: “es obvio que en este siglo la guerra mediática es uno de los métodos más fuertes; de hecho, puede alcanzar un ratio del 90% del total de la preparación para nuestras batallas”, no podía imaginar el grado de cumplimiento de tal vaticinio. (Akil, 2010)

Las nuevas tecnologías son uno de los factores estratégicos que han sabido explotar las organizaciones terroristas con multitud de finalidades, desde el reclutamiento, la propaganda, la financiación, el adiestramiento, la incitación o provocación a realizar acciones terroristas, hasta el acopio y difusión de información con finalidad terrorista.

La determinante campaña antiterrorista que siguió a los atentados del 11S provocó un cambio de estrategia por parte de los grupos terroristas que supieron ver en el ciberespacio, el nuevo campo de batalla. El endurecimiento del control por parte de

los servicios de información y contraterrorismo sobre los sitios web que les servían de plataforma hizo que las redes sociales, entre otras, se presentasen como una nueva alternativa a los medios tradicionales online.

Al-Qaeda e ISIS son las organizaciones más activas en el uso de las nuevas tecnologías. De hecho, la primera ha tenido presencia en Internet desde los años 90 y desde el año 2011 ambas tienen cuenta en redes sociales como Twitter. El Estado Islámico (DAESH o ISIS) tiene en las redes sociales su mayor escaparate mediático. Al mismo tiempo, Al-Qaeda en la Península Arábiga (AQAP), Hezbolá, Hamas y el Frente Al-Nusra tienen también destacada presencia en Twitter.

Si bien Al-Qaeda ha sido pionera, DAESH ha superado con creces la actividad de esta en la red, dando un salto cualitativo: "mientras Al-Qaeda y sus afiliados veían internet como un lugar donde diseminar anónimamente material o realizar encuentros en un lugar oscuro, el DAESH ha aprovechado la red como un ruidoso canal en el cual promocionarse, intimidar a la gente y radicalizar a sus nuevos reclutas. Las acciones llevadas a cabo en las redes plantean, así, todo un reto para los servicios de información y contraterrorismo, que se incrementa con la proliferación de nuevas tecnologías y smartphones" (Hannigan, 2014).

Como parte de la acción contraterrorista conjunta, miles de cuentas han sido rastreadas y clausuradas, a la vez que se abrían otras nuevas, provocando una espiral que parece tener difícil solución.

Existen elementos que convierten a España en objetivo del terrorismo internacional: la relativa cercanía a regiones inestables como el Sahel, la posible radicalización de los emigrantes, tanto de primera como de segunda generación, el hecho de que los grupos fundamentalistas islámicos presenten a este país como parte del imaginario del Islam, así como su decidida implicación en la lucha contraterrorista.

El uso de las nuevas tecnologías, con la finalidad última de cometer una acción terrorista al uso o en la modalidad de ciberataque, por parte de los grupos terroristas, es un problema transnacional que exige una acción coordinada e integrada entre los diferentes estados que conforman el sistema interestatal.

Sin embargo, a la ausencia de una gobernanza global de Internet, se suma otra gran dificultad a la hora de establecer una estrategia global contra este fenómeno, que es la necesidad de conocimientos técnicos para la investigación eficaz de estos delitos, así como la homologación de los procedimientos utilizados para obtención de información y garantizar su validez para sostener la imputación en el posterior proceso penal.

Por otro lado, una estrategia eficaz contra la yihad cibernética precisa de una cooperación policial ágil e implicación de todos los actores relevantes en el asunto, Estados miembros de las principales Organizaciones Internacionales, servicios policiales, de inteligencia y del ámbito de la ciberdefensa, jueces y fiscales, compañías proveedoras de servicios de tecnologías de la información, etc. (Enríquez, 2013).

2. ÁMBITOS DE ACTUACIÓN TERRORISTA

Internet y, en concreto, las redes sociales y las aplicaciones de mensajería privada en terminales móviles se han convertido en una poderosa herramienta para los grupos

extremistas, no solo como amplificadores de sus campañas de propaganda (incluidos el reclutamiento, la radicalización y la incitación al terrorismo) sino también como medio para la financiación, adiestramiento, planificación (tanto por medio de comunicaciones secretas, como mediante la información de dominio público), la ejecución y los ataques cibernéticos. La promesa de que la participación en la yihad electrónica es tan válida como la lucha sobre el campo de batalla, ha convertido las plataformas en un terreno abonado al que es muy difícil poner coto.

2.1. PROPAGANDA

Estos, a través de mensajes, ficheros de video, revistas, presentaciones, tratados, audio virtuales o incluso juegos de video, instruyen de una manera práctica o ideológica, justifican y promueven acciones terroristas.

Desde el año 2007, con la proliferación de las redes sociales, contenidos de distribución restringida que se entregaban en mano o a través de dispositivos de almacenamiento de información, desaparecen progresivamente. Facebook, Tumblr, Twitter, Youtube, Rapidshare o Instagram, junto con los blogs, salas virtuales de charla, revistas en línea y foros, se convierten en los canales más importantes para los grupos terroristas, de difusión de manuales de fabricación de armas, guerra psicológica o captación.

Esta propaganda puede tener como audiencia objetivo los partidarios u opositores, la comunidad internacional o las víctimas de las acciones terroristas.

2.1.1. Reclutamiento

Un reclutamiento dirigido a ganar el apoyo de las personas más receptivas a la propaganda, es decir, los grupos más vulnerables y marginados de la sociedad, como son los menores. Explota los sentimientos de injusticia, exclusión o humillación.

Factores como la edad o el género son tenidos en cuenta por la propaganda terrorista además de las circunstancias sociales o económicas.

Los foros de acceso restringido constituyen un medio para que los reclutas conozcan y puedan apoyar a organizaciones terroristas, así como colaborar con estas en acciones directas.

2.1.2. Incitación

Entendida como “una estrategia que utilizan comúnmente las organizaciones terroristas para aumentar el apoyo a su causa y llamar a la acción violenta”, su criminalización presenta controversia en algunos países en cuanto a los límites del derecho a la libertad de expresión contemplados en el Pacto Internacional de Derechos Civiles y Políticos.

Como veremos en el siguiente capítulo, el artículo 5 del Convenio Europeo para la Prevención del Terrorismo, del Consejo de Europa, insta a la prohibición de la incitación a la comisión de una acción terrorista: “siendo importante diferenciar la propaganda terrorista y la incitación en sí, sin menoscabar los derechos a la libertad de expresión, asociación y religión”.

2.1.3. Radicalización

Se trata del proceso de adoctrinamiento al que sigue la transformación de los reclutas en individuos decididos a pasar a la acción violenta. Se puede considerar que el reclutamiento, la radicalización y la incitación son fases o estadios previos a la comisión de una acción terrorista.

Cualquier musulmán que decida hacer "la yihad contra el enemigo electrónicamente es considerado, en un sentido u otro, un muyahidín en tanto que reúne las condiciones de la yihad y la intención sincera y el objetivo de servir al islam y defenderlo, aun cuando está lejos del campo de batalla". Esto ha favorecido el surgimiento de la figura del "lobo solitario" o individuo que, sin pertenecer necesariamente a organización terrorista alguna, se encomienda a esta idea para cometer acciones terroristas (Weinmann, 2014).

2.2. FINANCIACIÓN TERRORISTA

La recaudación de fondos a través de las redes sociales y otras plataformas virtuales se realiza generalmente a través de cuatro vías: recaudación directa (a través del envío masivo de correos electrónicos dirigidos a simpatizantes para obtener donaciones); comercio electrónico (a través de servicios de pago en línea que ofrecen ficheros de audio o video y libros); herramientas de pago online (uso fraudulento o robo de de tarjetas de crédito, etc.) y recaudaciones a través de donaciones a instituciones benéficas legítimas o víctimas de la infiltración terrorista.

2.3. ADIESTRAMIENTO

A modo de campo de entrenamiento virtual, a través de manuales en línea, documentos de audio o video, proporcionan instrucciones, en formato multimedia, sobre cómo enrolarse en una organización terrorista, cómo fabricar explosivos, armas de fuego, etc. y cómo realizar acciones terroristas. Estos materiales, constituyen herramientas para facilitar las actividades de contrainteligencia y las técnicas de cifrado para incrementar el nivel de seguridad de las comunicaciones.

2.4. PLANIFICACIÓN

Es difícil encontrar una operación contraterrorista en la que no se haya utilizado la tecnología de Internet, especialmente en la preparación de una acción, seleccionar un potencial objetivo o realizar actos preparatorios como la reunión de información de acceso público o, en relación con el objetivo seleccionado, mapas o instalaciones, o incluso la que figura en Facebook, Twitter, YouTube, Flickr, etc.

Son comunes las "comunicaciones secretas preparatorias" con una simple cuenta de correo electrónico y un "buzón compartido". Además utilizan software para enmascarar la dirección IP o reencaminar las comunicaciones por diferentes servidores y cifrar los datos de tráfico relativos a los sitios web utilizados. Así mismo utilizan la esteganografía: el ocultamiento de mensajes, por ejemplo, en imágenes.

2.5. EJECUCIÓN

La utilización de Internet facilita la ejecución de acciones con finalidad terrorista, al reducir las probabilidades de detección y el anonimato, ofreciendo infraestructura logística. Por ejemplo, la coordinación de la ejecución de acciones terroristas concretas o las amenazas terroristas, difundidas a través de Internet para generar en la audiencia pánico o miedo.

2.6. CIBERATAQUES

Entendidos como "la explotación deliberada de redes informáticas como medio para lanzar un ataque. Suelen estar destinados a perturbar el funcionamiento normal de computadoras, servidores o la infraestructura subyacente, mediante el uso de técnicas de piratería informática, virus informáticos, programas maliciosos, flooding (saturación) y cualquier otro medio de acceso no autorizado".

3. INSTRUMENTOS JURIDICOS INTERNACIONALES Y REGIONALES DE LOS QUE ESPAÑA FORMA PARTE

3.1. ORGANIZACIONES INTERNACIONALES

El marco jurídico internacional de lucha contra el terrorismo en Internet está constituido por diversas fuentes, entre las que se encuentran las resoluciones de la Asamblea General y el Consejo de Seguridad de la ONU, los tratados, la doctrina legal y el derecho internacional consuetudinario. Las resoluciones del Consejo de Seguridad pueden imponer obligaciones jurídicamente vinculantes para todos los Estados miembros. Igualmente, la Asamblea General ha aprobado varias resoluciones sobre terrorismo que, sin embargo, no son vinculantes.

Así mismo, los Estados se obligan, jurídicamente, en base a instrumentos bilaterales o multilaterales sobre terrorismo. Es importante tener en cuenta que son los propios Estados quienes deben de enjuiciar a los responsables de actos terroristas en territorio propio, ya que los tribunales internacionales carecen, por lo general, de dicha competencia[1].

3.1.1. Resoluciones de la ONU

Ya en el año 2006, la Asamblea General, con unanimidad de los Estados miembros, aprobó la Estrategia Global contra el Terrorismo, a través de la Resolución 60/288, en la cual estos resolvieron: "condenar de una manera firme, inequívoca y sistemática el terrorismo, adoptar medidas urgentes para prevenir y combatir el terrorismo, admitir que la cooperación internacional debe ajustarse al derecho internacional y cooperar con las Naciones Unidas para luchar contra el terrorismo en Internet y utilizar, así mismo, la red como instrumento para evitar la propagación de este fenómeno".

Por otro lado, existen diversas resoluciones del Consejo de Seguridad, aprobadas en la última década, que llaman a la cooperación en esta materia. Así, las Resoluciones

1 Actualmente solo el Tribunal Especial para el Líbano (Resolución del CS de la ONU 1757/2007) tiene competencia limitada sobre el delito de terrorismo.

1373 y 1566 de los años 2001 y 2004, respectivamente, requieren a todos los Estados miembros para que adopten medidas legislativas, y de otro tipo, para luchar contra el terrorismo al mismo tiempo que les exhortan a aplicar los convenios y protocolos internacionales que más adelante se mencionan.

En la misma línea, se aprobaron las Resoluciones 1624 del año 2005 y 1963 del año 2010. La primera de ellas, relativa a la glorificación e incitación de actos terroristas por Internet, insta a todos los Estados a que adopten medidas legislativas para prohibir la inducción a la perpetración de una acción terrorista. La segunda Resolución se centra en la utilización de las nuevas tecnologías de la información y las comunicaciones para el reclutamiento, incitación, financiación, planificación y preparación de actividades terroristas.

Finalmente, la Resolución 2178, del 24 de septiembre de 2014, exhorta a los Estados miembros a adoptar todas las medidas legales necesarias para impedir la circulación de terroristas o de grupos terroristas, mediante controles fronterizos de documentos de identidad y de viaje; utilización de procedimientos de evaluación del riesgo y control de pasajeros con base empírica; agilizar el intercambio de información operativa; prevenir la radicalización y reclutamiento de combatientes terroristas extranjeros; la financiación del terrorismo y el adiestramiento en técnicas de terrorismo.

En el apartado 6 de la referida resolución, se exige a los Estados miembros que creen los instrumentos legislativos necesarios para:

"Enjuiciar y sancionar a los nacionales que se desplacen a terceros países con el propósito de cometer, planificar o preparar actos terroristas o participar en ellos, o proporcionar o recibir adiestramiento con fines terroristas. Y a los que provea o recauden fondos, o coadyuven de alguna forma, para financiar viajes y desplazamientos a otros países para cometer actos terroristas o proporcionar o recibir adiestramiento".

3.1.2. Instrumentos Universales

Actualmente, los instrumentos legales universales no definen los delitos terroristas con arreglo al derecho internacional, tan solo contemplan la obligación de los Estados a penalizar dicha figura y establecer mecanismos de cooperación internacional para enjuiciar o extraditar a los implicados en delitos de terrorismo.

No existe ningún convenio universal que trate específicamente la prevención y la represión del uso de Internet con fines terroristas. De esta forma, serán los acuerdos bilaterales y multilaterales las únicas herramientas de cooperación internacional, hasta tanto en cuanto no se logre un convenio universal general sobre la materia.

3.2. INSTRUMENTOS EN ORGANIZACIONES REGIONALES

3.2.1. Consejo de Europa

En el año 2001, en el seno de esta Organización Internacional de carácter regional, se firmó el Convenio sobre la Ciberdelincuencia, que constituye la única herramienta jurídicamente vinculante, de carácter multilateral, que aborda la comisión de actos delictivos en Internet. Este tiene como finalidad la armonización de las legislaciones de los países firmantes tanto respecto al delito cibernético como al de terrorismo, la

mejora de los mecanismos de detección, investigación y persecución de estos delitos a través de la cooperación internacional.

Así, podríamos destacar la obligación de los Estados firmantes de legislar para exigir a los proveedores de servicios de Internet la conservación de los datos durante 90 días, con carácter renovable, si media una petición de conservación de los responsables de la investigación mientras se sustancia el correspondiente mandamiento judicial. Igualmente, se confiere al registro e intervención de los datos almacenados una protección similar a las pruebas tangibles conforme a la legislación nacional correspondiente.

En el mismo sentido, exige la facilitación de los datos relativos a abonados de estos proveedores de servicios para establecer la identidad del responsable de una acción terrorista a través de Internet. Como puede ser la ubicación física de este, datos relativos al tráfico de las comunicaciones o la interceptación de las mismas de acuerdo con las respectivas legislaciones nacionales.

Finalmente, en el seno del Consejo de Europa, se elaboró el Protocolo adicional al citado Convenio, sobre la penalización de actos xenófobos o racistas, que facilita la persecución del terrorismo a través de Internet, con la finalidad de incitar a la comisión de actos violentos por motivos de raza, color, etnia, religión, etc.

Por otro lado, el Convenio Europeo para la Prevención del Terrorismo constituye un instrumento específico para este fenómeno y obliga a los países que se adhieran, miembros o no del Consejo de Europa, a tipificar como delitos la incitación pública, el reclutamiento y adiestramiento a través de Internet. De igual modo, contempla medidas de cooperación internacional como el intercambio de información.

3.2.2. Unión Europea

En la Decisión Marco del 13 de junio de 2002, 2002/475/JAI, el Consejo de la UE abordaba la armonización de la definición del delito de terrorismo en todos los Estados miembros. Debido al aumento del terrorismo de corte yihadista, se modificó en el año 2008 para introducir disposiciones específicas sobre la incitación pública, reclutamiento y adiestramiento terrorista, a través de la Decisión Marco 2008/919/JAI del Consejo de la Unión Europea, de 28 de noviembre de 2008.

Esta, en concordancia con la anteriormente citada resolución 1624 (2005) del Consejo de Seguridad de la ONU, establece un marco de referencia para la persecución de la difusión de propaganda e instrucciones para la confección de artefactos explosivos a través de la red, siempre y cuando tengan como finalidad la comisión de actos terroristas.

A raíz de los atentados de París de enero de 2014, y más recientemente de los de noviembre de 2015, se han aprobado, en el seno de la UE, una serie de medidas para luchar contra este concreto fenómeno:

1. “Una nueva Decisión Marco que crea un marco legal para la cooperación contra el terrorismo y la Estrategia de Seguridad Interior.
2. Desarrollo del SIS (Schengen Information System), sistema de intercambio de información, y del Mecanismode Protección Civil.

3. Creación de la RAN (Radicalisation Awareness Network), red de expertos multidisciplinar que identifica casos de buenas prácticas para prevenir la radicalización en los entornos sociales identificados como de riesgo.
4. Reforzamiento de la cooperación entre Europol y otras agencias europeas y mejora del intercambio de información sobre la compraventa ilegal de armas.

La propuesta más importante es la culminación de la adopción de un registro PNR (Passenger Name Record), para mejorar el control de los pasajeros que ingresan o salen de la UE" (Narrillos, 2015).

3.2.3. España

A nivel nacional existe un marco en forma de acuerdo entre los dos principales partidos nacionales, y a los que se han ido sumando otros, ante la necesidad de afianzar la unidad de los demócratas frente al terrorismo. Se trata del "Acuerdo para afianzar la unidad en defensa de las libertades y en la lucha contra el terrorismo", que ha sido reeditado el pasado 14 de noviembre tras los atentados del 13 del mismo mes en París.

Este contemplaba, como medidas principales a adoptar, las modificaciones legislativas penales o el Plan Estratégico Nacional de Lucha contra la Radicalización Violenta (PEN-LCRV), aprobado por Acuerdo de Consejo de Ministros el 30 de enero de 2015, que relaciona tres ámbitos de actuación, interno, externo y ciberespacio, coherente con la Estrategia de Seguridad Nacional Española aprobada en 2013, y tres áreas funcionales según el momento en que debe hacerse frente al fenómeno de la radicalización: antes, durante y después.

Como se ha mencionado anteriormente, en virtud de la Resolución 2178, del Consejo de Seguridad de las Naciones Unidas, se ha adaptado la legislación penal nacional a través de la LO 2/2015 de 31 de marzo de 2015.

Según el Grupo de Estudios en Seguridad Internacional, "esta reforma constituye un gran paso para la prevención de la difusión del terrorismo yihadista a través de redes sociales, entre otros medios, tipificando tanto la difusión de ideas incitadoras como el adiestramiento en técnicas para la comisión de cualquier delito de terrorismo. También supone un importante apoyo legislativo la penalización de los desplazamientos a territorios controlados por organizaciones o grupos terroristas, para recibir adiestramiento o adoctrinamiento, tipificándolos como delito".

Las modificaciones derivadas de esta Resolución afectan a los delitos de terrorismo contenidos en los artículos 571 al 580 del Código Penal, destacando la introducción expresa de la configuración de los delitos informáticos como delitos de terrorismo cuando se cometan con finalidad terrorista. "Se tipifica como delito el que, con esta finalidad de adiestrarse, tenga en su poder documentos, archivos o acceda de forma habitual a servicios de comunicación vía internet o electrónica cuyos contenidos sean idóneos para incitar a la incorporación a organizaciones o grupos terroristas o a colaborar con cualquiera de ellos".

Igualmente, "en relación a los delitos de enaltecimiento o actos de humillación, descrédito o menosprecio a las víctimas del terrorismo, cabe la adopción judicial de medidas cautelares en el caso de que dichos delitos se cometan mediante servicios o contenidos accesibles a través de internet o de servicios de comunicaciones

electrónicas. Se podrá ordenar la retirada de los contenidos, la supresión de los enlaces y la prohibición de acceso a dichos contenidos ilícitos".

Por otro lado, la reciente Ley 36/2015, de 28 de septiembre, de Seguridad Nacional, constituye un marco de referencia para hacer frente a esta amenaza a través del ciberespacio, "considerando la Seguridad Nacional como un objetivo compartido por las diferentes administraciones, estatal, autonómica y local, los órganos constitucionales, en especial las Cortes Generales, el sector privado y la sociedad civil, dentro de los proyectos de las organizaciones internacionales de las que formamos parte".

Otra de las novedades en esta materia es la Ley Orgánica 13/2015, de 5 de octubre, de modificación de la Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica.

Entre las importantes novedades procesales que contiene destaca la adaptación a las formas de delincuencia ligadas al uso de las nuevas tecnologías. Así:

- "Toda medida de intervención deberá responder al principio de especialidad: la actuación de que se trate deberá tener por objeto el esclarecimiento de un hecho punible concreto, prohibiéndose las medidas de investigación tecnológica de naturaleza prospectiva.
- Las medidas de investigación tecnológica deben satisfacer los principios de idoneidad, excepcionalidad, necesidad y proporcionalidad, cuya concurrencia debe encontrarse suficientemente justificada en la resolución judicial habilitadora.
- Se autoriza la intervención y registro de las comunicaciones de cualquier clase que se realicen a través del teléfono o de cualquier otro medio o sistema de comunicación telemática, lógica o virtual.
- Se establece un plazo de tres meses como duración máxima inicial de la intervención, hasta un máximo de 18 y se regula el registro de dispositivos informáticos de almacenamiento masivo y el registro remoto de equipos informáticos.
- Para asegurar la autenticidad e integridad de los soportes puestos a disposición del juez, se impone la utilización de un sistema de sellado o firma electrónica que garantice la información volcada desde el sistema central.
- Por último, se regula la figura del agente encubierto informático, que requiere autorización judicial para actuar en canales cerrados de comunicación y que a su vez, requerirá una autorización especial para intercambiar o enviar archivos ilícitos por razón de su contenido en el curso de una investigación".

3.3. PROBLEMÁTICA JURÍDICA Y PROCESAL ENTRE MARCOS NORMATIVOS

En este apartado, se pretende poner de manifiesto los problemas derivados de los diferentes enfoques legales a nivel internacional que dificultan la persecución del terrorismo yihadista en Internet. Teniendo en cuenta que no solo basta con adaptar la legislación nacional a esta concreta amenaza, sino que es necesaria una armonización internacional, debido al carácter transnacional de la misma.

Actualmente y debido a la dimensión de la evolución de la amenaza en los últimos meses, los Estados están legislando a marchas forzadas en este ámbito, pero todavía muchos de ellos carecen de legislación específica en el uso de Internet con fines terroristas.

Sin embargo, a nivel internacional, no existe un instrumento amplio y vinculante que establezca normas definitivas sobre la regulación de las actividades en Internet. Por ello, la mayoría de países han optado por lidiar con el fenómeno mediante la combinación de leyes penales generales y específicas sobre terrorismo y ciberdelincuencia, ya existentes en sus respectivos ordenamientos. Así, las diferentes fiscalías, hacen uso de las disposiciones normativas que se adaptan mejor al caso.

Máxime, ante la ausencia de una definición universalmente aceptada de terrorismo como la que existe acerca de la pornografía infantil. (Conway, 2007).

3.3.1. Ámbito Penal

Ante la ausencia de imposición, por parte de los instrumentos internacionales contra el terrorismo, de la obligación de legislar específicamente contra el uso de Internet con fines terroristas, los Estados han optado por recurrir a sus respectivos códigos penales, además de invocar los instrumentos universales que tratan la amenaza.

El principal problema radica en la diferente o ausente penalización de conductas o figuras relacionadas con el terrorismo yihadista en muchos países donde se encuentran ubicados los servidores o los proveedores de servicios de Internet.

Sin este requisito de la doble incriminación, muchas investigaciones y procesos penales iniciados en un Estado se frustran. Por tanto, es fundamental que cuando se tipifiquen estas conductas se utilicen figuras delictivas lo más similares posible para evitar diferentes interpretaciones.

3.3.2. Ámbito Procesal

Los instrumentos jurídicos universales citados en el punto uno, prevén la extradición, la asistencia judicial recíproca, la remisión de actuaciones penales y traslado de las personas condenadas, la ejecución recíproca de sentencias, el embargo preventivo y decomiso de activos. Sin embargo, la incompatibilidad de los diferentes sistemas penales ha puesto en evidencia, en la práctica, que las solicitudes de asistencia judicial recíproca o de extradición habían sido rechazadas o ejecutadas con demora por no satisfacer, entre otros, el requisito de la doble incriminación.

El primer obstáculo surge en relación al intercambio de información confidencial entre los diferentes países. Los órganos jurisdiccionales que compartan datos reservados exigen que sus destinatarios mantengan las debidas garantías de la que gozan en sus respectivos países.

Otro, es el concepto de soberanía de los Estados. En algunos casos estos pueden percibir una investigación en su territorio como una injerencia. Tal es el caso del registro a distancia de un ordenador ubicado en otro país. Otro aspecto controvertido es la retención y entrega de la información vinculada a actividades realizadas por Internet por una persona

relacionada con el terrorismo. Así como información sobre cuentas bancarias, tarjetas de crédito, información sobre el uso por parte de esta de servicios de comunicaciones por Internet como el correo electrónico, Skype, VoIP, redes sociales u otros sitios web.

Uno de los problemas principales es la ausencia de un marco internacional o convenio sobre la retención de estos datos por parte de los proveedores de servicios de Internet. A nivel internacional, no existe ningún plazo establecido de referencia, por lo que es muy complicado llegar a tiempo para salvaguardar la información cuando se trate de investigaciones que afecten a más de un país[2].

Cuestión también importante es la observancia de los requisitos probatorios de los sistemas legales de los países afectados. La información proporcionada a través de la cooperación policial, con métodos de registro, vigilancia e interceptación, encubiertos o intrusivos, altamente especializados debe ser coherente con la jurisdicción que finalmente entenderá del asunto. Por ejemplo la cadena de custodia de la intervención física de los ordenadores para análisis forense o los informes periciales realizados por expertos en la lucha contraterrorista.

Otra cuestión que plantea problemas es la competencia sobre el delito en cuestión, cuando el terrorista está ubicado en un país pero utiliza, para la su comisión, sitios de Internet o servicios de proveedores ubicados en otro. En este caso, ante la ausencia de normas vinculantes en el derecho internacional para dirimir los conflictos de competencia, los Estados se basan en cuestiones como la nacionalidad de este, el lugar de la comisión o el lugar donde se encuentran los testigos y las pruebas para reivindicar su competencia.

Por otro lado, muchos países condicionan la cooperación en esta materia a la existencia de tratados internacionales o, al menos, de reciprocidad con el país requirente, en materia de asistencia judicial recíproca y extradición.

Finalmente, otro gran obstáculo existente en la persecución del terrorismo y del uso de las nuevas tecnologías con el mismo fin son las legislaciones nacionales de protección de datos y de la privacidad.

4. RESPUESTA POLICIAL: INSTRUMENTOS DE COOPERACIÓN POLICIAL INTERNACIONAL Y PROCEDIMIENTOS DE INVESTIGACIÓN. CONTRIBUCIÓN MILITAR

4.1. COOPERACIÓN POLICIAL INTERNACIONAL

Ante la ausencia de un instrumento universal que aborde el uso de las nuevas tecnologías con fines terroristas, para facilitar la cooperación judicial y policial internacional en esta materia, se hace necesario recurrir a otros instrumentos no específicos, ya existentes, en el ámbito de las organizaciones de las que España forma parte o con los países con que mantiene acuerdos multilaterales o bilaterales.

2 Tan sólo la UE ha establecido tal obligación, de 6 meses a 2 años, pero existe inseguridad jurídica mientras no haya un período de retención estándar.

4.1.1. Instrumentos de cooperación no específicos

Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional: Se trata de la principal herramienta para la cooperación entre Estados en materia de delincuencia organizada pero que, dadas las características que reúnen las organizaciones terroristas, es posible su aplicación a los casos de terrorismo internacional.

Convenio sobre la Ciberdelincuencia y otros: Contiene mecanismos de cooperación en materia policial y judicial, como pueden ser la comunicación oficiosa de información entre Estados, miembros o no miembros del Consejo de Europa, adheridos.

Además de este, el Convenio Europeo para la Prevención del Terrorismo del Consejo de Europa, el Convenio Europeo sobre Extradición, el Convenio Europeo sobre cooperación judicial en materia penal y el Acto 2000/C 197/01, de 29 de mayo de 2000, del Consejo de la UE, relativo a la asistencia judicial en materia penal entre Estados de la UE, podrían ser de aplicación para la cooperación internacional en materia de terrorismo internacional que tenga relación con el uso de Internet.

4.1.2. Otros instrumentos de cooperación

Orden de Detención Europea: Establece, dentro del marco Schengen, la obligatoriedad para los Estados de la UE de detener y trasladar a un presunto terrorista al Estado requirente, en base al principio de reciprocidad. Esta incluye a los propios nacionales cuando el hecho ha sido cometido en otro país miembro.

Orden Europea de Investigación (OEI). Consiste en un procedimiento simplificado para obtención y remisión, establecido en virtud de la Directiva del Parlamento Europeo y del Consejo 2014/41/CE, de documentos, objetos, datos de usuarios de Internet, etc. que puedan servir de elementos de prueba.

Red 24/7 del Consejo de Europa: Establecida en virtud del artículo 35 del Convenio sobre la Ciberdelincuencia del Consejo de Europa, establece la disponibilidad de contactos, las 24 horas del día los siete días de la semana, para casos de ciberdelincuencia.

En el seno del Consejo de Europa se creó, también, el Comité Especial de Expertos sobre la evaluación de medidas contra el blanqueo de dinero y financiación del terrorismo.

Plan de acción de la Unión Europea: Centro de Ciberdelincuencia: Los Estados miembros encomendaron a la Comisión Europea y a Europol la tarea de crear un Centro Europeo de Ciberdelincuencia. Este se dedica a la lucha contra las organizaciones criminales que cometen ciberdelitos graves.

A nivel europeo, los diferentes cuerpos policiales colaboran en mejorar las técnicas y procedimientos de investigación a través de internet, desarrollando incluso herramientas propias que se puedan emplear por todos los investigadores.

4.1.3. Instrumentos de cooperación internacional entre agencias y cuerpos de seguridad

Grupo Egmont de unidades de inteligencia financiera: Se trata de un organismo internacional cuya finalidad es la promoción y optimización de la cooperación de las

unidades de inteligencia financiera en la persecución del blanqueo de capitales y financiación del terrorismo.

Organización Internacional de Policía Criminal. (INTERPOL): Para el intercambio y análisis de información entre los países miembros, a través de su sistema I-24/7 y el programa de ciberdelincuencia para coordinar las operaciones internacionales, prestar asistencia en investigaciones, asistencia en caso de ciberataques, etc.

Oficina Europea de Policía (EUROPOL): Responsable de reforzar la cooperación entre las Fuerzas y Cuerpos de Seguridad de los Estados miembros de la UE en materia de terrorismo y delincuencia organizada, a través de Internet. Proporciona: base de datos sobre ciberdelincuencia**,** programa de evaluación de la amenaza de la delincuencia organizada por Internet, incluido terrorismo, y los ataque a redes electrónicas (iOCTA), sistemas de denuncias on-line de delitos cometido por Internet (ICROS) y el Foro de Expertos Forenses (iFOREX).

Europol ha puesto en marcha un nuevo equipo policial especialmente formado para bloquear y cerrar todas aquellas cuentas en plataformas sociales que estuvieran vinculadas con el terrorismo islámico (Casciani, 2015). También se ha puesto en marcha el Centro Europeo Contra el Terrorismo (ECTC), al mando de un Coronel de la Guardia Civil, con la finalidad de mejorar el intercambio de información tanto operativa como estratégica en el ámbito de esta amenaza.

Eurojust: Como unidad de cooperación judicial de la UE, en colaboración con Europol, promueve el intercambio de información entre las diferentes autoridades judiciales en investigaciones y enjuiciamientos relacionados con el terrorismo, emisión y ejecución de órdenes de detención europea, etc.

Una herramienta útil en este ámbito es el Terrorism Convictions Monitor (TCM)[3], es un informe interno de Eurojust que, entre otras cuestiones, facilita a los miembros de la justicia ejemplos de sentencias y de interpretación de la legislación de la UE contra el terrorismo. Especialmente útil en el tratamiento desde el punto legal de los foreign fighters.

Cooperación oficial y oficiosa: A pesar de la existencia de estos instrumentos mencionados, es necesaria para una cooperación internacional eficaz la existencia de una autoridad central que asuma esa responsabilidad, con capacidad legal, autonomía e iniciativa suficiente para liderar la coordinación entre autoridades policiales, servicios de inteligencia (incluida la financiera), autoridades judiciales e incluso aquellas unidades pertenecientes al ámbito de la ciberdefensa. Con procedimiento claros y simplificados que incluyan mecanismos oficiales y oficiosos.

Aunque los canales oficiales ofrecen mayor garantía en cuanto al éxito de las investigaciones y enjuiciamiento de este tipo de delitos, los procedimientos oficiosos son mucho más ágiles y exigen menos burocracia. Y dado que el factor tiempo es fundamental para la disponibilidad de datos digitales, este será el medio más habitual, principalmente a través de oficiales de enlace (en cuerpos policiales extranjeros o Agregadurías de Interior) e investigaciones conjuntas (equipos conjuntos de investigación de duración limitada en el seno de EUROPOL).

3 Implementado por la Decisión 2005/671/JAI del Consejo de la Unión Europea.

4.2. PROCEDIMIENTOS Y HERRAMIENTAS DE INVESTIGACIÓN

Las actuales investigaciones de la actividad terrorista yihadista en Internet se basan en una combinación de métodos de investigación tradicionales y los ideados específicamente en relación con las pruebas digitales, que exigen estar familiarizados con las técnicas especializadas de investigación en un entorno virtual.

4.2.1. Comunicaciones por Internet

Telefonía de voz por Internet (VoIP): A través de estas aplicaciones los terroristas pueden comunicarse en tiempo real, incluyendo conversaciones a través de video o texto, y permiten compartir ficheros. Destacan los proveedores de servicios VoIPSkype y Vonage, etc., los cuales convierten el sonido analógico en formato digital comprimido con lo que no requieren de un gran ancho de banda.

Las dificultades en la investigación se deben a que la facturación se realiza en base al volumen de paquetes de datos transmitidos en lugar de las señales analógicas como se hace con las llamadas tradicionales telefónicas, con lo que se hace más complicada la determinación de hora de llamada o ubicación de los usuarios. Si, además, las llamadas se realizan a través de redes punto a punto (P2P) o mediante el cifrado de datos de llamada, la dificultad es aún mayor.

Sin embargo, el volumen del tráfico de datos en un momento dado, así como la dirección IP, dirección electrónica o los datos de pago del usuario proporcionados por el proveedor de servicios de Internet, pueden servir para la identificación de este.

Correo electrónico: Proporciona un medio encubierto de comunicación. Un correo electrónico estándar se compone de encabezado del sobre, encabezado del mensaje, cuerpo del mensaje y ficheros adjuntos.

El encabezado del sobre suele proporcionar información sobre los servidores por los que ha pasado el mensaje hasta su destino y la información sobre la dirección IP del remitente. Esta es más difícil de manipular que la del encabezado del mensaje.

Para reducir (o eliminar) la posibilidad de detección, los terroristas suelen utilizar el procedimiento de comunicación a través de mensajes no enviados, accesibles desde la carpeta de borrador y al que pueden acceder múltiples destinatarios con una contraseña compartida de acceso a la cuenta. Si además utilizan un terminal de acceso público, como un cibercafé, las posibilidades de identificación de estos se reducen.

Así mismo, emplean técnicas de anonimato ocultando la dirección IP del remitente o utilizando servidores de correo que mantienen el anonimato, sesgando la información de identificación del encabezado del sobre.

Para intercambiar información de promoción terrorista, emplean software de esteganografía Camouflage para ocultar datos dentro de imágenes en formato JPEG y GIF y software de WinZip para cifrar ficheros, que se remiten adjuntos a las comunicaciones por correo electrónico.

Servicios de mensajería en línea y chats (salas de charla): Los primeros son un medio de comunicación bilateral, mientras que los segundos lo son para un grupo

de personas. La inscripción para el uso de estos servicios se basa en información no verificada que proporciona el propio usuario.

Aunque algunos proveedores de servicios registran la dirección IP de acceso, no guardan, generalmente, la información intercambiada durante una sesión y para su recuperación posterior será necesario el análisis forense del disco duro de al menos uno de los usuarios.

Las salas de charla en línea a través de contraseña, que son frecuentemente utilizadas por los terroristas y simpatizantes, ofrecen mayores posibilidades de obtención de pruebas documentales, incluso la infiltración en las mismas, a través de la figura del agente encubierto, con la limitación de no incurrir en la comisión de la infracción penal de inducción al delito.

Redes de intercambio de ficheros y almacenamiento en nube: Los más utilizados son los sitios web Fileshare, Rapidshare o Dropbox, que proporcionan la posibilidad de cargar, compartir y acceder a ficheros multimedia a través de la red. Estas permiten el cifrado y el anonimato mediante la tecnología P2P y el Protocolo de Transferencia de Ficheros (FTP).

En el marco de una investigación, alguna de estas redes puede dejar rastro de transferencias de efectivo o pagos, útiles con fines de identificación de usuarios.

Con respecto a la computación en nube, proporciona acceso remoto a programas y datos almacenados o ejecutados en los servidores de datos de terceros. Esta permite el almacenamiento, compartición y distribución de documentación en línea.

Al reducir la cantidad de información almacenada localmente en los dispositivos físicos, dificulta la recuperación de pruebas con fines investigativos, que aumenta si, además, los servidores de datos están ubicados en otro país.

Cifrado de datos y anonimato: A través de un algoritmo matemático y una clave de cifrado pueden proteger la información del conocimiento de terceros. Con un equipo físico, un software o una combinación de ambos son capaces de cifrar datos “en reposo”, contenidos en discos duros de los ordenadores, unidades externas de memoria o smartphones, y los datos “en tránsito” a través de Internet, como los anteriormente mencionados telefonía VoIP y correo electrónico.

“Los más habituales son los programas informáticos WinZiP, Truecrip y Pretty Good Privacy (PGP) para la protección de contraseñas y para el cifrado o esteganografía el Camouflage. También hacen uso del software Detekt que identifica malware de vigilancia sobre sus actividades en la Red.

Otra técnica que utilizan para ocultar la identidad de los usuarios es la de ocultación de la dirección IP de origen, usurpar la de otro terminal o redirigir la información a una dirección IP oscurecida”.

Una de las maneras de salvar esta dificultad es la aprehensión del equipo informático encendido y con los ficheros abiertos, salvando las claves criptográficas. Para ello, es necesario recurrir a técnicas tradicionales, como el seguimiento de la actividad del sospechoso para elegir el momento idóneo de la detención.

Redes inalámbricas (Wi-Fi): que permiten el acceso a Internet con ordenador u otro dispositivo (teléfono móvil, tabletas, etc.) a través de una señal de radio. Pueden facilitar el acceso a través de contraseña o abierto. El acceso anónimo a estas permite a los terroristas desvincular su actividad en Internet con sus datos identificativos.

En la actualidad existen empresas proveedoras de servicios, como la española FON, que permite que los usuarios inscritos compartan su ancho de banda de red wi-fi con otros abonados en cualquier parte del mundo, a través de una aplicación que localiza esas redes.

Por tanto, las dificultades de investigación son considerables, tanto en lo que respecta a la posibilidad de interceptación de las comunicaciones como de la localización de los transmisores.

Red TOR (The Onion Router): Conocida como la red oscura en la que los mensajes intercambiados no revelan la dirección IP de los usuarios. Los mensajes no viajan entre iguales (Peer to Peer, P2P), sino a través de una serie de "routers cebolla" a modo de encaminadores de los mismos, cedidos por diferentes organizaciones o individuos con ancho de banda suficiente. (Gellman y Rich, 2013).

4.2.2. Investigación Tipo

Enfoque sistemático de las investigaciones: Internet ofrece herramientas útiles, como datos y servicios disponibles, que se pueden emplear en una investigación tipo contra el terrorismo yihadista a través de la red.

La necesidad de establecer un procedimiento sistemático de investigación a través de Internet, ha llevado a INTERPOL y EUROPOL, con la participación de la Universidad de Dublín y su Máster en Informática Forense y Ciberdelincuencia, a elaborar un protocolo para este fin, ya llevado a la práctica por muchos Estados miembros, y que establece los hitos básicos para realizar este tipo de investigaciones.

Valor identificativo de una dirección IP: Toda comunicación de Internet tiene asociada una IP (Protocolo Internet) que identifica la red y el dispositivo desde el cual se ha realizado ese acceso. Las direcciones IP pueden ser dinámicas, facilitada por un proveedor de servicios temporalmente y para una sesión en línea, o estáticas, como las direcciones de los sitios web.

En las primeras de ellas, se puede identificar la región o país desde donde un ordenador se conecta a Internet y a través del correspondiente mandamiento judicial, y previo requerimiento para la conservación de los datos digitales hasta que se libere este, se puede solicitar a un proveedor de servicios de Internet que identifique la cuenta de un abonado que, en un momento dado, estaba vinculada a una determinada dirección IP.

En las investigaciones relacionadas con sitios web es necesario identificar qué dirección IP estática corresponde al nombre del dominio en cuestión. Para ello, se utilizan aplicaciones basadas en un protocolo TCP (Protocolo de Control de Transmisión) de petición respuesta como who.is o nslookup. Sin embargo, la información registrada es la que previamente ha proporcionado el titular o puede encontrarse el dominio arrendado a otro titular diferente.

Es importante tener en cuenta que toda actividad investigadora puede a su vez ser monitorizada por terceros. Por ello, no debe realizarse desde equipos oficiales.

Aplicaciones especializadas de investigación: Existen diversas aplicaciones de búsqueda especializadas, que pueden ser utilizadas con fines identificativos si se dispone de una adecuada formación técnica. Por ejemplo, “Ping”, la cual permite conocer si un ordenador está conectado a Internet en un momento dado, a través del envío de una señal o “Traceroute”, que facilita la ruta entre dos ordenadores conectados en red permitiendo determinar así su ubicación física.

Existen otros programas que, con las limitaciones legales de cada país, permiten el acceso a dispositivos e interceptación de las comunicaciones. Son los denominados caballos de Troya, que sirven para la obtención de información o el control remoto de un ordenador, una vez se ha introducido en este.

Por otro lado, los capturadores de teclado (hardware o software), pueden obtener información de la actividad de un teclado, como pueden ser las contraseñas de acceso, comunicaciones o actividad en un sitio web. Por su parte, los “Sniffers” o rastreadores de paquetes de datos, permiten la obtención de información de la fuente y el contenido de las comunicaciones.

Preservación y recuperación de datos: Para su uso con fines probatorios, la recuperación de datos digitales almacenados deben realizarse respetando las técnicas forenses que permitan su admisibilidad en juicio y como en cualquier investigación, con escrupuloso respeto de la cadena de custodia.

En cuanto a la preservación de datos, si se interrumpe el suministro eléctrico de un ordenador los datos volátiles de los discos de almacenamiento y memoria RAM pueden verse alterados, perdiéndose información sobre usuarios, contraseñas o mensajes instantáneos. Sin embargo, los datos no volátiles almacenados en discos duros, unidades de memoria portátiles, dispositivos de almacenamiento flash y discos de compresión (discos ZIP), no se ven afectados por esta circunstancia.

En el documento publicado por UNODC: “Manual de buenas prácticas para incautarse de pruebas electrónicas”, se incluye una guía de este proceso.

Con respecto a los teléfonos inteligentes, tabletas, etc., se utiliza el mismo procedimiento pero debe evitarse el apagado del dispositivo por el requerimiento posterior de contraseña o pérdida de datos.

Los exámenes que se realicen sobre los datos deben de realizarse sobre copias de los elementos de prueba originales, utilizando herramientas forenses como EnCase, de la empresa Guidance Software o FTK (Forensic Tool Kit). Existen otros programas gratuitos y sería conveniente utilizar dos diferentes para crear duplicados y asegurar la preservación de datos.

Validación de la autenticidad de las pruebas digitales: Para el enjuiciamiento de un caso de uso de Internet con fines terroristas es imprescindible garantizar la integridad de las pruebas digitales y, especialmente, la cadena de custodia.

EnCase, por ejemplo, crea una imagen duplicada de los datos y analiza el dispositivo para capturar ficheros ocultos o borrados. También crea y asigna un identificador

único (valor hash) a las pruebas digitales, con la finalidad de validar su autenticidad. La coincidencia de los valores hash confirma la no manipulación de estas y permite trabajar sobre los datos de la copia con validez judicial.

Informes periciales de inteligencia: La información obtenida acerca de la actividad terrorista, en general, y en Internet, en particular, puede servir de punto de partida para el inicio de una investigación policial y posteriormente judicial, una vez trabajada y elaborada, generando el correspondiente informe de inteligencia.

Además, puede servir de prueba en un posterior juicio en determinados ordenamientos jurídicos, entre los que se encuentra el español, convirtiéndose así en un informe pericial de inteligencia y los funcionarios policiales que lo redactan se convierten, por tanto, en peritos de inteligencia.

En la mayoría de Estados existe la dicotomía entre la confidencialidad de la identidad de la fuente, informador o colaborador y el derecho de los procesados a un juicio justo y que se respete el principio de contradicción o de conocer y rebatir las pruebas que se presenten en su contra. Y más a tenor de la escasa protección que, legislaciones como la española, otorgan al testigo protegido.

En otros muchos países la inteligencia procedente de fuentes anónimas no es admisible como elemento de prueba salvo si es complementada con otras pruebas o corroborada por funcionarios policiales de un determinado rango.

4.2.3. Colaboración con otros actores

Fuerzas Armadas y Centro Nacional de Inteligencia: En el ámbito de las ciberamenazas se plantean las siguientes dudas: por un lado, qué constituye un acto de ciberguerra y, por otro, la atribución de la responsabilidad del mismo, con lo cual queda la duda de qué organización debería tomar la iniciativa cuando ocurren cibereventos y no está claro quién está detrás de ellos. “Si se trata de una cuestión de seguridad nacional o un asunto militar dependiendo de si detrás de ellos se encuentran delincuentes, hackers, terroristas o estados paria. La evidencia necesaria para probarlo ante un tribunal exigirá mucho más”. (Caro, 2010)

Más allá de la cibercriminalidad, en el ámbito de la ciberdefensa, se precisa una definición más clara de qué se entiende por acto de ciberguerra y quién es el responsable del mismo. Mientras no se establezca una cooperación internacional adecuada en ciberinvestigación, la capacidad de atribuir un ciberataque a un autor concreto será difícil. (Caracuel, 2002)

Teniendo en cuenta el tratamiento que desde el Gobierno de la nación se ha dado al terrorismo yihadista, a través del mencionado “Acuerdo para afianzar la unidad en defensa de las libertades y en la lucha contra el terrorismo”, parece evidente que se ha basado eminentemente en un enfoque penal, que implica especialmente a Fuerzas y Cuerpos de Seguridad, Jueces y Fiscales.

No obstante, pese a que la investigación de esta amenaza desde el punto de vista de la seguridad interior compete a las FCSE, bajo la coordinación del CITCO, en la práctica, Fuerzas Armadas y CNI colaboran, desde el punto de vista técnico y de intercambio

de información, para poner a los terroristas a disposición de las autoridades judiciales nacionales[4].

Sector privado: la colaboración por parte de estos es fundamental para una respuesta oportuna y eficaz contra el terrorismo yihadista y el uso que sus miembros hacen de Internet. A pesar de que ya colaboran de facto, tienen la obligación moral de hacer más. (Ben Solomon, 2014)

Proveedores de servicios de Internet juegan un papel crucial en la conservación y cesión de datos digitales y en el rigor con el que los exigen a sus usuarios para hacer uso de sus servicios.

Por otro lado, los sitios web o plataformas que hospedan contenido generado por los usuarios, como YouTube, con casi ocho millones de usuarios al mes, puede hacer de barrera a los contenidos de corte yihadista al permitir que los usuarios denuncien aquellos que inciten, promuevan, etc. Lo mismo se podría decir de Twitter o facebook. (Chimbelu, 2015)

Conway (2007) sostiene que los buscadores de Internet (Google, Yahoo, etc.) constituyen un puente entre los contenidos de Internet y el usuario, por tanto, estos pueden bloquear y eliminar los resultados de búsqueda relacionados con posibles organizaciones terroristas.

Por otro lado, existen servicios de monitorización como Search for International Terrorist Entities (SITE), que funcionan como un servicio de inteligencia y recibe sus ingresos de suscripciones. O Internet Haganah, que detecta y bloquea el acceso a contenidos extremistas islámicos y se financia por aportaciones de una red de voluntarios. (Eunjung, 2005).

5. CONCLUSIONES

Es evidente que la Comunidad Internacional se encuentra, más que nunca, bajo la amenaza del terrorismo yihadista quién, con la promesa de que la participación en la yihad electrónica es tan válida como la lucha sobre el campo de batalla, ha encontrado en las nuevas tecnologías su mejor instrumento para llegar a los jóvenes, como principal audiencia objetivo.

A marchas forzadas los gobiernos y las principales empresas se replantean la necesidad de monitorizar dichas redes, con la clara finalidad de evitar la radicalización de los jóvenes y prevenir ataques terroristas. Lejarza (2015) defiende que la tarea se presenta complicada, debido a la pericia que han alcanzado dichas organizaciones para evadir cualquier intento de control por parte de los servicios de inteligencia.

Además, y pese al carácter transnacional de este terrorismo, no existe ni una definición oficial del término terrorismo, ni ningún convenio universal que aborde espe-

4 Destacan los Comités Especializados de Ciberseguridad y de Situación bajo la dependencia directa del Consejo de Seguridad Nacional. Cada país tiene sus CERT (Equipo de Respuesta a Emergencias Informáticas) para hacer frente a los ciberataques (que pueden ser de origen terrorista). En OTAN, existe el NATO Computer Incidents Response Capability Technical Centre (NCIRC-TC). A nivel europeo la European Union Agency for Network and Information Security (ENISA) intercambia información de interés para la prevención de ciberataques.

cíficamente la prevención y la represión de este asunto desde un perspectiva global, más allá de diversas resoluciones del Consejo de Seguridad de la ONU, que obliga a los Estados miembros a cooperar sin reservas en esta materia.

Ante la ausencia de una legislación armonizada en materia de Ciberseguridad, se han elaborado convenios o convenciones de carácter regional, en el seno del Consejo de Europa o la Unión Europea, que pretenden regular y uniformar criterios con más o menos acierto. Esto ha provocado que los Estados hayan adoptado soluciones "ad hoc", aplicando una combinación de leyes penales generales con otras específicas de ciberdelincuencia y contraterrorismo.

No obstante, a raíz de los recientes atentados de París y Bruselas, en el seno de la UE ha habido avances importantes, destacando, entre otros, medidas como la adopción del registro y control de pasajeros, Passenger Name Record (PNR), con origen o destino en la UE.

España ha sido de los países que más medidas ha adoptado durante el productivo, desde el punto de vista legislativo, año 2015, en relación a la prevención del impulso del terrorismo yihadista a través de redes sociales, comunicaciones electrónicas o creación de páginas web o foros, "penando tanto la difusión de ideas incitadoras como el adiestramiento en técnicas para la comisión de cualquier delito de terrorismo. Destacando, entre otras, la introducción expresa de la configuración de los delitos informáticos como delitos de terrorismo".

Ya en el ámbito penal y procesal es donde mayores disfunciones se evidencian por la incompatibilidad de los diferentes sistemas penales internacionales. Así, las solicitudes de asistencia judicial recíproca o de extradición se rechazan sistemáticamente o se ejecutan con demora por no satisfacer, entre otros, el requisito de la doble incriminación o del respeto a la cadena de custodia correspondiente.

Además, la ausencia de un acuerdo o convenio sobre los plazos de conservación de los datos por parte de los proveedores de servicios de Internet, a nivel internacional, dificulta recuperar la información en investigaciones que afecten a más de un país. Los métodos de registro, vigilancia e interceptación o los informes periciales deben reunir los requisitos procesales de países con muy diferentes niveles de exigencia en este ámbito.

Finalmente, se carece de normas internacionales vinculantes para dirimir las cuestiones de competencia cuando el terrorista está ubicado en un país y el servidor de Internet en otro distinto, o por el diferente grado de protección que cada país otorga a los datos personales y la privacidad, principal obstáculo para la investigación.

En el ámbito de la respuesta a este fenómeno, se hace patente la necesidad de incrementar la formación, especialmente en investigación e informática forense, y continuar con la colaboración, ya iniciada, con universidades y expertos. Los procedimientos de investigación precisan de una normalización internacional. Estos se basan en una combinación de métodos tradicionales con otros técnicos que se encuentran disponibles en la propia Red pero que no están homologados y su validez jurídica se basa en el informe técnico pericial del perito correspondiente.

Por todo ello, las herramientas legales, de cooperación policial y procedimientos técnicos de investigación, debido a la multitud de actores implicados, la dificultad de

coordinación y la rapidez con que evolucionan las nuevas tecnologías y procedimientos utilizados por las organizaciones terroristas hacen que la capacidad de respuesta sea inferior a la de la amenaza.

BIBLIOGRAFÍA

Akil A. (2010). The virtual Jihad: An Increasingly Legitimate Form of Warfare. Combating Terrorist Center. Extraído el 06 de noviembre de 2015 de: https://www.ctc.usma.edu/posts/the-virtual-jihad-an-increasingly-legitimate-form-of-warfare.

Ambos K. (2012). Creatividad judicial en el Tribunal Especial para el Líbano: ¿Es el terrorismo un crimen internacional? Revista de derecho penal y criminología. Universidad Nacional de Educación a Distancia. 3ª Época, nº 7, p. 173.

Ben Solomon, A. (2016). Jihadist Groups Using Facebook, Twitter to Spread Their Mesage. The Jerusalem Post. Extraído el 14 de abril de 2016 de: http://www.jpost.com/Middle-East/Jihadist-groups-using-Facebook Twitter-to-spread their-message-363050

Caracuel Raya, M. A. (2002). La OTAN ante la cumbre de Praga. Real Instituto Elcano. ARI Nº 104, p. 2

Caro Bejarano, M. J. (2010). Alcance y ámbito de la seguridad nacional en el ciberespacio. Ciberseguridad. Retos y amenazas a la seguridad nacional en el ciberespacio.. Cuadernos de Estrategia. Instituto Español de Estudios Estratégicos, nº 149., p. 78

Casciani, D. (2015). Islamic State web accounts to be blocked by new police team, BBC News, Junio 2015. Extraído el 14 de abril de 2016 de: http://www.bbc.com/news/world-europe-33220037

Chimbelu, Ch. (2015). Social network intensify efforts to crackdown on jihadists. DW. Extraído el 19 de abril de 2016: http://www.dw.de/social-networks-intensify-efforts-to-crackdown-on-jihadists/a-18318205

Conway, M. (2007). Terrorism and Internet governance: core issues. Disarmament Forum. Vol. 3, pp 27-31.

Enríquez González, C. (2012). Estrategias internacionales para el ciberespacio. Ministerio de Defensa: Instituto Español de Estudios Estratégicos. Extraído el 13 de noviembre de 2015 de: http://dialnet.unirioja.es/servlet/oaiart?codigo=4540379

Eunjung C., A. (2005). Watchdogs seek out the web´s bad side. Washington Post. Extraído el 9 de abril de 2016 de: www.washingtongpost.com/wpdyn/contetn/article/2005/04/24/AR2005042401473.html

Gellman B., Timberg C. & Rich S. (2013). Secret NSA documents show campaign against Tor encrypted network. The Washington Post.4 de Octubre de 2013. Extraído el 23 de abril de: https://www.washingtonpost.com/world/national-security/secret-nsa-documents-show-campaign-against-tor-encrypted-network/2013/10/04/610f08b6-2d05-11e3-8ade- 1f23cda135e_story.html

Hannigan, R. (2014). The Web is a Terrorist's Command and Control Network of Choice. Extraído el 13 de noviembre de 2015 de: http://www.ft.com/cms/s/2/c89b6c58-6342-11e4-8a63-00144feabdc0.html#axzz3eBXGu0zh.

Lejarza, E. (2015). Terrorismo Islamista en las Redes-La Yihad Electrónica. Documento de Opinión. Instituto Español de Estudios Estratégicos 2015, nº 100, p. 18.

Narrillos, E. (2016). El Parlamento aprueba la directiva sobre registro de datos de pasajeros (PNR). En Portada. Extraído el 14 de abril de 2016 de: http://www.europarl.europa.eu/news/es/news-room/20160407IPR21775/El-Parlamento-aprueba-la-directiva-sobre-registro-de-datos-de-pasajeros-%28PNR%29.

Stalinsky, Steven y Sosnow. (2015). Encryption Technology Embraced By ISIS, AlQaeda, Other Jihadis Reaches New Level With Increased Dependence On Apps, Software –Kik, Surespot, Telegram, Wickr, Detekt, TOR Parte IV. Extraído el 08 de abril de 2016 de: http://cjlab.memri.org/latest-reports/encryption-technology-embraced-by-isis-al-qaeda-other-jihadis-reaches-new-level-with-increased-dependence-on-apps-software-kik-surespot-telegram-wickr-detekt-tor-part-iv-f/.

Weinmann, G. (2014). New Terrorism and New Media. Wilson Center Research Series. Vol. 2. Extraído el 13 de noviembre de 2015 de: https://www.wilsoncenter.org/publication/new-terrorism-and-new-media

PUBLICACIONES OFICIALES

ASOCIACIÓN INTERNACIONAL DE ABOGADOS, DIVISIÓN PRÁCTICA FORENSE. Report of theTask Force on Extraterritorial Jurisdiction. 2008.

COMISIÓN EUROPEA. GRUPO DE EXPERTOS EN MATERIA DE RADICALIZACIÓN VIOLENTA: Radicalisation processes leading to acts of terrorism 2008.

EC-COUNCIL PRESS. Computer Forensics: Investigating Data and Image Files. Nueva York: 2010

EUROJUST: Foreign Fighters: Eurojust´s View son the Phenomenom and the Criminal Justice Response. Updated Report. Enero 2015

EUROPOL. Comunicado de la Oficina de Europea de Policía. 3 de enero de 2011. Extraído el 8 de enero de 2016 de: www.europol.europa.eu/content/press/cybercrime-presents-major-challenge-law-enforcement-523.

FISCALÍA GENERAL DEL ESTADO. Memoria de la Fiscalía General del Estado 2015. Madrid: 2015.

GOBIERNO DE ESPAÑA. Estrategia de Ciberseguridad Nacional. Madrid: 2013

GOBIERNO DE ESPAÑA. Estrategia de Seguridad Nacional. Un proyecto compartido. Madrid: 2013.

GRUPO DE ESTUDIOS EN SEGURIDAD INTERNACIONAL. La reforma de los delitos de terrorismo mediante la Ley Orgánica 2/2015. Granada: 2015.

MINISTERIO DE INTERIOR. Estrategia Integral Contra el Terrorismo Internacional y la Radicalización (EICTIR). Madrid: 2012.

MINISTERIO DE INTERIOR. Plan Estratégico Nacional de Lucha contra la Radicaliza-

ción Violenta (PEN-LCRV). Madrid: 2015.

MINISTERIO DE LA PRESIDENCIA. Acuerdo para afianzar la unidad en defensa de las libertades y en la lucha contra el terrorismo. Madrid: 2015.

OFICINA DE LAS NACIONES UNIDAS CONTRA LA DROGA Y EL DELITO. Compendio de casos relativos a la lucha contra el terrorismo. 2010.

OFICINA DE LAS NACIONES UNIDAS CONTRA LA DROGA Y EL DELITO. El uso de Internet con fines terroristas. Viena: 2013.

OFICINA DE LAS NACIONES UNIDAS CONTRA LA DROGA Y EL DELITO Manual de buenas prácticas para incautarse de pruebas electrónicas. UNODOC. Viena: 2013.

OFICINA DE LAS NACIONES UNIDAS CONTRA LA DROGA Y EL DELITO. Preguntas frecuentes sobre cuestiones de derecho internacional de la lucha contra el terrorismo. Viena: 2009.

OFICINA DEL ALTO COMISIONADO DE LAS NACIONES UNIDAS PARA LOS DERECHOS HUMANOS. Los derechos humanos, el terrorismo y la lucha contra el terrorismo. Septiembre 2008

OFICINA DE PROGRAMAS JUDICIALES. Investigations Involving the Internet and Computer Networs. Instituto Nacional de Justicia. Departamento de Justicia de Estados Unidos: 2007.

Fecha de recepción: 18/11/2016. Fecha de aceptación: 20/12/2016

DARK WEB Y DEEP WEB COMO FUENTES DE CIBERINTELIGENCIA UTILIZANDO MINERÍA DE DATOS

EVA MARTÍN IBÁÑEZ

DOCTORA EN CIENCIAS DE LA INFORMACIÓN

RESUMEN

Deep Web es la parte más grande de Internet, cuyos contenidos no pueden indexar los buscadores web convencionales; puede servir para actividades legales e ilegales. Dark Web ocupa las zonas más oscuras de Deep Web y requiere de herramientas específicas de acceso. Ambas constituyen una importante fuente de ciberinteligencia, especialmente sobre amenazas, vulnerabilidades y riesgos. La minería de datos, en sentido amplio, puede ayudar a encontrar sentido a las ingentes cantidades de datos existentes en Deep Web y Dark Web. Esas técnicas permiten el análisis cuasi automático de conjuntos de datos enormes y complejos para desvelar patrones e identificar tendencias.

Palabras clave: Deep Web, Dark Web, ciberinteligencia, darknet, minería de datos, knowledge discovery

ABSTRACT

The Deep Web is the largest part of the Internet, whose contents are not indexed by standard search engines; it can be used for legal and illegal activities. The Dark Web takes up the darkest corners in the Deep Web and requires specialized tools to access. Both represent an important source of cyber intelligence, mainly in regards to threats, vulnerabilities and risks. Data mining can help to make sense of massive amounts of data from the Deep Web and the Dark Web. Those techniques allow quasi-automatic analysis of large and complex data sets to unveil patterns and identify trends.

Keywords: Deep Web, Dark Web, cyber intelligence, darknet, data mining, knowledge discovery

1. INTRODUCCIÓN

La minería de datos (*data mining*), en sentido amplio, puede ayudar a mejorar las capacidades de lucha contra el crimen organizado y el terrorismo, porque contribuye a reducir la sobrecarga informativa y cognitiva de las personas. Ofrece un gran potencial a la hora de extraer conocimiento implícito en los datos. Miembros de los cuerpos y fuerzas de seguridad y de la comunidad de la inteligencia pueden beneficiarse de estos métodos y técnicas para encontrar sentido a los datos y para presentar los resultados eficazmente a los decisores.

La tremenda cantidad de datos, además en rápido crecimiento, excede la capacidad de comprensión humana. Eso conduce a la situación actual, rica en datos pero pobre en información. Esa brecha entre datos e información, que está en constante

ensanchamiento, requiere el desarrollo de herramientas potentes que puedan convertir los datos en perlas de conocimiento (Han, Kamber y Pei, 2012, p. 5).

Deep Web y Dark Web constituyen unas fuentes muy relevantes para la labor de la ciberinteligencia. Allí es posible encontrar información valiosa sobre amenazas, vulnerabilidades y riesgos. El problema es que las cantidades de datos que hay que recopilar y analizar son tan enormes que sobrepasan los métodos tradicionales de análisis y vigilancia.

Una posible solución a la sobrecarga informativa es recurrir a herramientas como la minería de datos o el Knowledge Discovery in Database (KDD). Esas técnicas permiten el análisis cuasi automático de conjuntos de datos enormes y complejos para identificar tendencias y patrones previamente desconocidos. El objetivo final es generar información válida para tomar decisiones o para aportar como prueba en un procedimiento judicial.

Las páginas siguientes están estructuradas en varios apartados. Para empezar, se aclaran las definiciones de Deep Web, Dark Web, Surface Web, ciberespacio y minería de datos. Seguidamente, se comenta por qué interesa analizar Deep Web y Dark Web desde el punto de vista de la seguridad. Después se explican qué dificultades presentan estos ámbitos para la minería de datos. A continuación figuran ejemplos de uso, clasificados en tres grandes áreas: las arañas (*crawlers*) para Deep Web, los sistemas de detección y prevención de intrusiones (IDPS) y la detección de comunidades. Las conclusiones ponen el cierre.

2. DEFINICIONES

El ciberespacio designa el “dominio global y dinámico compuesto por las infraestructuras de tecnología de la información –incluida Internet–, las redes y los sistemas de información y de telecomunicaciones” (Gobierno de España, 2013, p. 9). Dentro de Internet, existe una cierta confusión de términos. A menudo Deep Web (Internet Profunda) y Dark Web (Internet Oscura) se usan indistintamente. Sin embargo, es conveniente diferenciarlos.

Deep Web es aquella parte de Internet que no es accesible a los motores de búsqueda basados en enlaces como Google. La única manera de acceder a ella es introducir una consulta directa en un formulario de búsqueda web. De esa forma, se pueden recuperar contenidos dentro de una base de datos que no está enlazada (Pederson, 2013, p. 2). En cambio, Surface Web (Internet Superficial) sí es accesible a través de técnicas de rastreo web basadas en enlaces, que conducen a datos localizables vía hiperenlaces desde la página principal de un dominio. Buscadores como Google, Bing o Yahoo pueden encontrar esos datos en la Internet Superficial (Pederson, 2013, p. 2).

Deep Web se refiere a cualquier contenido de Internet que, por diversos motivos, no puede ser indexado por los buscadores. Incluye páginas web dinámicas, sitios bloqueados (como los que requieren responder un CAPTCHA para acceder), sitios no enlazados, sitios privados (que necesitan credenciales para entrar), contenidos que no son HTML, contextuales o con scripts, y redes de acceso limitado. Las redes de acceso limitado están formadas por nombres de dominio registrados en sistemas de nombres de dominio (DNS) no gestionados por ICANN (Internet Corporation for Assigned Names and Numbers) y por direcciones URL (Uniform Resource Locator) con dominios de

primer nivel o TLD (Top-Level Domains) no estandarizados que generalmente requieren un servidor DNS específico para resolver correctamente. Un ejemplo de redes de acceso limitado son los sitios con dominios registrados en sistemas distintos del estándar DNS, como los .BIT. Esos sitios no solamente escapan de las regulaciones impuestas por la ICANN, sino que, debido a su naturaleza descentralizada, son muy complicados de desviar a un sumidero. Bajo la categoría de redes de acceso limitado también se encuentran las Darknets o sitios alojados en infraestructuras que requieren el uso de software específico como Tor para acceder. Precisamente la mayor parte de las actividades de interés público dentro de Deep Web ocurren dentro de las Darknets (Ciancaglini, Balduzzi, McArdle y Rösler, 2015, p. 5).

Un estudio de 2001, cuando solo había unos tres millones de dominios en Internet, estima que el tamaño de Deep Web es aproximadamente entre 400 y 550 veces mayor que el de Surface Web. Por aquella época, Deep Web contenía 750 Terabytes de información frente a los 19 Terabytes de Surface Web, y el 95% de Deep Web era públicamente accesible, en el sentido de no requerir cuotas de suscripción (Bergman, 2001, p. 1).

Deep Web es la parte más grande de Internet y puede usarse para el bien y para el mal, para actividades legales y para actividades ilegales. Conviene saber que no todo es malo. Hay muchos aspectos buenos en Deep Web, incluyendo el derecho a la privacidad cuando se navega por Internet (Hawkins, 2016, p. 17).

Dark Web no es lo mismo que Deep Web. Dark Web se refiere a cualquier página web que se oculta a plena vista o que reside dentro de una capa pública pero separada de la Internet estándar. Por ejemplo, una página web que carece de enlaces de entrada, de manera que ni los usuarios ni los motores de búsqueda pueden localizarla (Pederson, 2013, p. 3). En definitiva, Dark Web es una parte de Deep Web. Si se adopta la metáfora de los túneles de una mina, Dark Web ocuparía las zonas más profundas de Deep Web que requieren herramientas o equipamiento altamente especializados para acceder a ellas. Reside en los subterráneos más profundos, y los dueños de los sitios tienen más razones para mantener sus contenidos ocultos (Ciancaglini et al., 2015, p. 6).

Las Darknets modernas necesitan software específico para usar la red distribuida. Hoy en día los ejemplos más notables son Tor, I2P (Invisible Internet Project) y Freenet. La arquitectura fluida de estas redes complica estimar su tamaño, pero parece que Tor es la más grande con I2P a bastante distancia. El resto son mucho más pequeñas en alcance y popularidad (Moore y Rid, 2016, p. 15).

Otros conceptos relacionados son Dark Net o Darknet, que frecuentemente se utilizan como equivalentes de Dark Web. En realidad, hay varias definiciones de Darknet (Fachkha y Debbabi, 2016, p. 1198). La primera es cualquier sistema de comunicación que opera furtivamente y oculta la identidad de sus usuarios, como pueden ser Freenet y BitTorrent. La segunda se refiere a servidores y programas que sirven para distribuir ilegalmente material protegido por derechos de autor, como las tecnologías P2P (Peer-to- Peer). La tercera definición remite a servidores configurados para atrapar adversarios y recopilar datos sospechosos. Este último tipo de Darknet funciona en modo pasivo sin interactuar con los atacantes; corresponde a dispositivos y servidores sin utilizar; también se conoce como Darkspace o como direcciones IP sin usar. En resumen, Darknet, según esa tercera acepción, es un sistema de monitorización con trampas que funciona de modo pasivo. Su tecnología está diseñada para inferir actividades y amenazas en Internet (Fachkha y Debbabi, 2016, p. 1223).

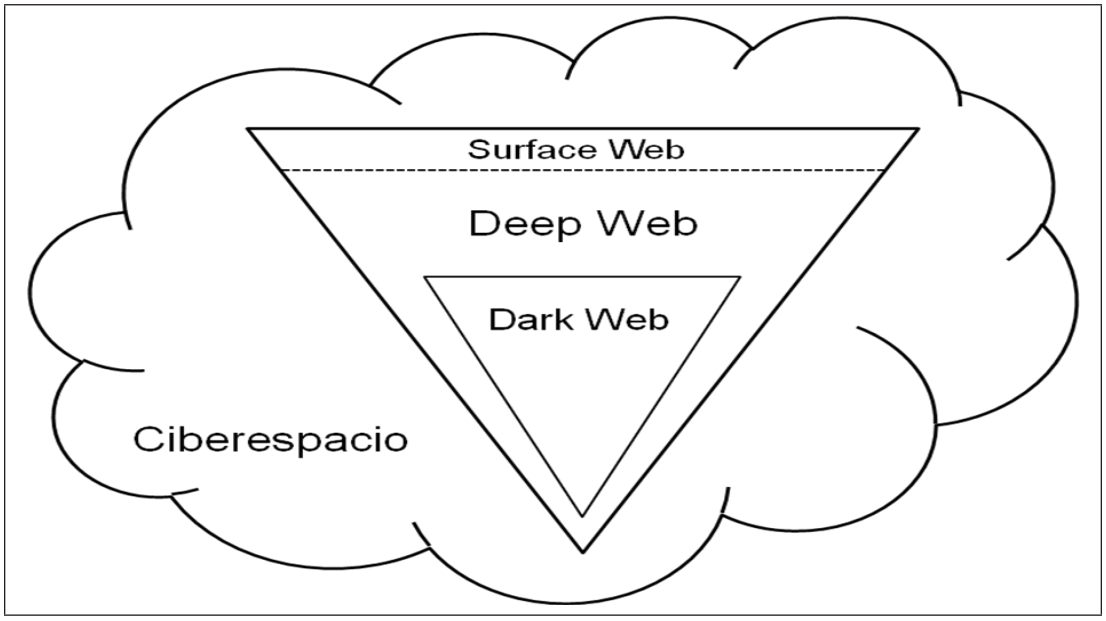

Figura 1. Ciberespacio, Deep Web y Dark Web. Fuente: Elaboración propia.

El tamaño de Darknet se estima en 270.000 direcciones IP (Internet Protocol) a mayo de 2015 (Nakao, 2016, p. 4). Los ataques en Darknet a través del puerto 23, que corresponde el servicio Telnet, se han disparado en 2015, según el NICT japonés (National Institut of Information and Communications Technology). El principal origen de dichos ataques son dispositivos IoT (Internet de las Cosas), con más de 150.000 direcciones IP atacantes y 361 modelos de dispositivos IoT observados en sólo cuatro meses (Nakao, 2016, p. 5).

Existen muchos motivos, aparte de comprar drogas, por los que la gente quiere mantenerse en el anonimato o instalar sitios en línea que no se puedan vincular con un lugar físico o con una entidad (Ciancaglini et al., 2015, p. 6). Por ejemplo, informantes o disidentes políticos pueden estar interesados en proteger sus comunicaciones, sobre todo en países con regímenes políticos represivos. Dark Web también es útil para periodistas y para activistas pro derechos humanos que en ciertos lugares del mundo pueden sufrir amenazas de cárcel o censura. Aunque se busquen soluciones para combatir las actividades ilegales y nefarias en Dark Web, eso no debería perjudicar las actividades legales y legítimas de libertad de expresión (Weimann, 2016, p. 43).

Finalmente, el término minería de datos a menudo se usa para referirse a todo el proceso de Knowledge Discovery in Database (KDD)[1]. Así, la minería de datos, entendida en sentido amplio, sería el proceso de descubrir conocimientos y patrones interesantes en grandes cantidades de datos. Las fuentes de datos pueden ser bases de datos, almacenes de datos, la web, otros repositorios de información o

1 Knowledge Discovery in Database (KDD) incluye varias etapas: Limpieza de datos (para eliminar datos inconsistentes y ruidosos); integración de datos (donde se pueden combinar varias fuentes); selección de datos (se recuperan de la base de datos los que son relevantes para el análisis); transformación de datos (los datos se agregan o se consolidan en formas adecuadas para realizar después el minado); minería de datos (proceso esencial en el que se aplican métodos de inteligencia para extraer patrones de datos); evaluación de patrones (para identificar aquellos patrones que son realmente interesantes y que suponen conocimiento); y presentación del conocimiento (mediante técnicas de visualización y representación para mostrar el conocimiento extraído a los usuarios) (Han et al, 2012, pp. 7-8).

datos transmitidos al sistema de forma dinámica (Han et al., 2012, p. 7). Abarca una amplia variedad de técnicas de diversos campos como la estadística, el aprendizaje automático (*machine learning*), el reconocimiento de patrones, las bases de datos, la recuperación de información, la visualización, los algoritmos o la computación de alto rendimiento, entre otros (Han et al., 2012, p. 23).

Muchas de esas técnicas de Knowledge Discovery se pueden aplicar a los estudios de seguridad, teniendo en cuenta sus peculiaridades. Las más empleadas se pueden clasificar en estas categorías: compartición de información, análisis de asociaciones criminales, clasificación y clusterizado del crimen, análisis de inteligencia y análisis espacio-temporal de delitos (Chen, 2012, p. 26).

3. POR QUÉ INTERESA

En los ámbitos de la seguridad y la defensa, Deep Web en general y Dark Web en particular constituyen una importante de fuente de ciberinteligencia, especialmente sobre amenazas, vulnerabilidades y riesgos.

El uso de Deep Web puede dividirse en dos clases: actividades legales y actividades ilegales. Con independencia de que el uso sea legal o ilegal, el acto de acceder a Deep Web siempre implica una acción deliberada (Hawkins, 2016, p. 7).

Aunque no lo parezca, hay muchas actividades legales que se desarrollan en Deep Web. Es un recurso útil para multitud de información. Por ejemplo, hay bases de datos con librerías académicas virtuales y con versiones antiguas de páginas web (Hawkins, 2016, p. 7). Junto a estos contenidos legales hay otros que son irregulares o que son completamente ilícitos.

Una muestra de los productos y servicios ilegales que están disponibles dentro de las Darknets abarca los siguientes: contenidos pirateados; drogas; dinero falsificado; productos de lujo robados; tarjetas de crédito y cuentas bancarias; robo de identidad; pasaportes y otros documentos oficiales; armas, munición y explosivos; servicios de mercenarios y asesinos a sueldo; contenidos de abuso sexual a menores; tráfico de seres humanos (adultos y menores); y tráfico de órganos (Goodman, 2015, pp. 201-204).

Un reciente estudio realizado con 300.000 direcciones de la red Tor revela que solamente algo más de la mitad (el 52,3%) están activas. Entre los sitios activos, el 56,8% están dedicados a actividades ilícitas (Moore y Rid, 2016, p. 21). Los contenidos se pueden clasificar en 13 categorías: armas, drogas, extremismos, finanzas, hacking, pornografía ilegal, nexos, otros ilícitos, sociales, violencia, otros lícitos, ninguno y desconocido.

- Armas: Armas y municiones.
- Drogas: Drogas ilegales o medicamentos ilícitos.
- Extremismos: Ideologías extremistas, incluyendo expresiones de apoyo al terrorismo, guías prácticas militantes y foros extremistas.
- Finanzas: Blanqueo de dinero, moneda falsificada y venta de cuentas y tarjetas de crédito robadas.
- Hacking: Hackers de alquiler y distribución de malware o ataques DDoS.

- Pornografía ilegal: Material pornográfico que involucra menores, violencia, animales o materiales obtenidos sin el consentimiento de los participantes.
- Nexos: Dedicados a enlaces con otros sitios ilícitos y recursos dentro de Darknets.
- Otros ilícitos: Materiales que no entran en las categorías anteriores pero que son problemáticos, como la venta de carnets y pasaportes falsificados.
- Sociales: Comunidades en línea para compartir material ilícito en forma de foros, redes sociales y tablones de mensajes.
- Violencia: Asesinos a sueldo e instrucciones sobre cómo realizar ataques violentos.
- Otros lícitos: Servicios legítimos, como contenidos de tipo ideológico o político, puntos seguros de entrega y recogida y repositorios de información.
- Ninguno: Sitios que son completamente inaccesibles o carecen de contenidos visibles, incluyendo aquellos que están en pruebas.
- Desconocido: Su naturaleza es difícil de determinar por ser contenidos ilegibles o dispersos.

Hay una manera de diferenciar entre sitios lícitos e ilícitos en Dark Web. Los sitios legítimos casi siempre identifican a sus operadores, mientras que los ilícitos los esconden. Los proveedores de servicios ilícitos se esconden detrás del anonimato o se aprovechan de las ventajas de seguridad de la plataforma (Moore y Rid, 2016, pp. 24-25).

La Figura 2 muestra la distribución de los contenidos en la red Tor.

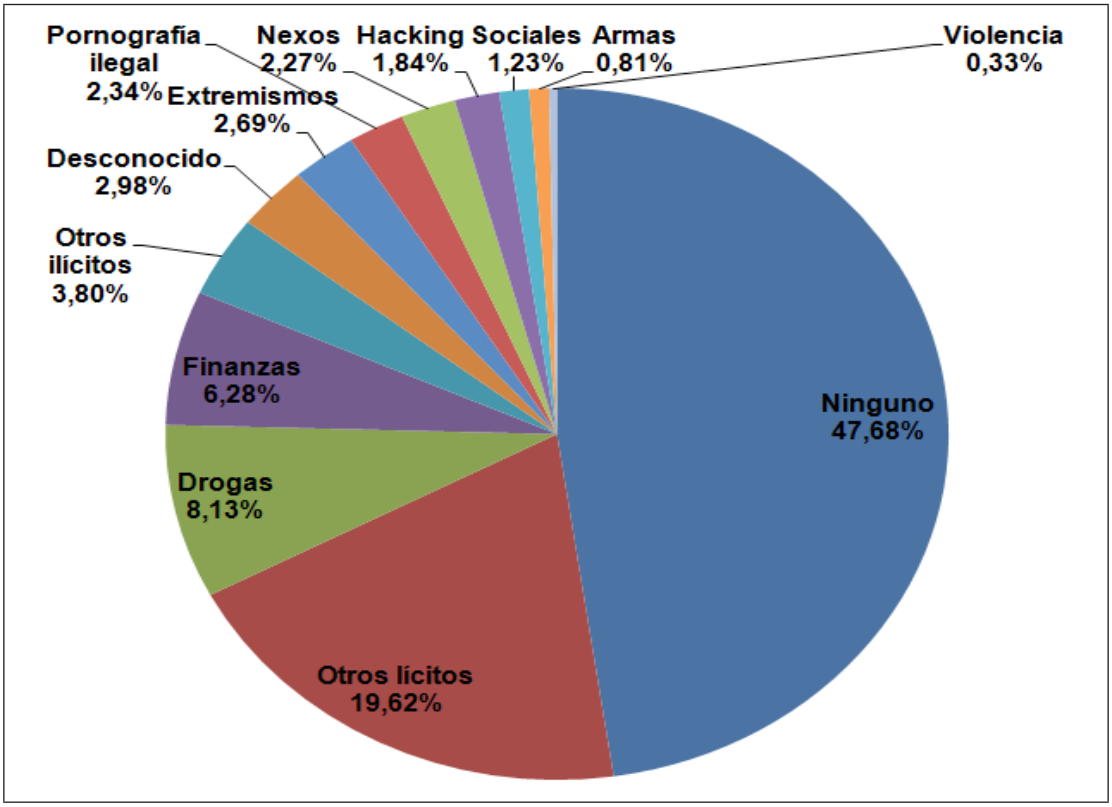

Figura 2. Contenidos en la red Tor. Fuente: Elaboración propia a partir de Moore y Rid, 2016, pp. 20-21.

En Dark Web, igual que en el mundo real, los delincuentes necesitan ser presentados y sus referencias deben ser comprobadas antes de poder realizar transacciones. La distribución de bienes y servicios está organizada alrededor de miles de salas de chat ilícitas y de foros mediante previa invitación. Los sitios ilícitos más exclusivos requieren contar con direcciones alfanuméricas secretas, que no están listadas en línea, sino que se pasan de persona a persona. Ciertos foros criminales impiden que los candidatos aspirantes entren en sus mundos clandestinos sin haber recibido la aprobación unánime por parte de los miembros más antiguos de la organización y transcurrido un periodo de espera de más de una semana (Goodman, 2015, p. 202).

Casi la mitad de los Estados miembros de la Unión Europea ha investigado actividades relacionadas con drogas o con pagos fraudulentos con tarjetas en Darknet, y más de un tercio de los países europeos ha indagado en actividades relacionadas con propiedad intelectual, tráfico de armas o cuentas bancarias comprometidas. Casi un tercio de los cuerpos policiales de la Unión Europea monitoriza activamente los mercados en Darknet, sobre todo para operaciones específicas en lugar de para recopilar inteligencia con carácter general. Una pequeña parte de los delincuentes activos en la Internet Oscura consigue explotar con éxito negocios que generan pingües beneficios. Es un mercado muy concentrado, donde el 1% de los vendedores acapara el 51,5% del total de las transacciones en Darknet (Europol, 2015, p. 52).

Dark Web ofrece recursos a los criminales para acceder a tutoriales, donde pueden adquirir instrucciones y comprar las herramientas necesarias para hackear ordenadores y cometer delitos, con un anonimato virtual. Esa parte del ciberespacio puede crear una desconexión mental entre el criminal, el delito y el mundo real, porque las víctimas no tienen rostro y no se emplea violencia directa. Ya no hace falta una banda, unas pistolas y un coche para robar un banco; cualquier individuo puede cometer el crimen desde su habitación con un simple ordenador portátil (UK Government Office of Science, 2015, p. 57).

Actividades delictivas, como el crimen organizado, el terrorismo o el espionaje, se desarrollan cada vez con mayor frecuencia en el ciberespacio a través de sofisticados procedimientos técnicos y operativos. Un ejemplo es “la internet oculta (deep web), donde se realizan actividades ilegales de todo tipo favorecidas por el anonimato del usuario” (Gobierno de España, 2016, p. 54).

Dark Web ha crecido significativamente en la última década. Los contenidos almacenados en las redes oscuras requieren software específico para acceder a ellas y, por tanto, quedan ocultas para la mayoría de los internautas y facilitan la navegación y las comunicaciones anónimas. Dark Web se ha convertido en una cadena de suministro madura que sostiene actividades cibercriminales, que incluye la venta de todo lo que un ciberdelincuente necesita para embarcarse en una actividad maliciosa. Además, esa misma cadena de suministro hace posible que el delincuente pueda vender lo que ha robado (UK Government Office of Science, 2015, p. 75).

Esas complejas cadenas de suministro para el cibercrimen pueden extenderse por todo el mundo, como Silk Road, y usar tecnologías anonimizadoras como Tor, que permiten que cualquier persona pueda comprar cualquier producto o servicio, desde software malicioso a tiempo de alquiler de una botnet (UK Government Office of Science, 2015, p. 76).

Los mercados ocultos o criptomercados son unas plataformas comerciales en línea que reúnen múltiples vendedores que ofrecen bienes y servicios generalmente ilegales. En ellos predomina la venta de estupefacientes y sustancias ilegales (Aldridge, Judith y Décary-Hétu, 2016, p. 1).

A principios de octubre de 2013, el principal mercado negro en línea, Silk Road, era desmantelado por el FBI. En pocas semanas sus vendedores se pasaban a los de la competencia o abrían sus propios negocios anónimos. A principios de noviembre de 2013 se inauguraba Silk Road 2.0, que acabó cerrando un año después. En pocos meses muchos mercados anónimos nuevos aparecieron, con distintos grados de sofisticación, duración y especialización. A la vez otros desaparecieron, ya fuera debido a detenciones o voluntariamente. El ecosistema de los mercados anónimos en línea ha evolucionado significativamente, comparado con la primera época cuando Silk Road casi era un monopolio. La facturación estimada de Silk Road oscilaba entre 1,1 y 1,2 millones de dólares al año. Por su parte, Silk Road 2.0 vendía unos ocho millones de dólares al mes antes de su clausura en noviembre de 2014 (Soska y Christin, 2015, p. 33 y 46).

Los mercados negros en Deep Web se sustentan en tres elementos tecnológicos. Criptodivisas como Bitcoin, que funcionan igual que el dinero en efectivo; la red Tor anonimiza el tráfico web; y los programas de cifrado PGP (Pretty Good Privacy) blindan los datos dentro de los mensajes de correo electrónico. El anonimato es esencial. La verdadera identidad de compradores y vendedores permanece oculta, y solo se les conoce por sus nombres de usuario (Hardy y Norgaard, 2015, p. 2).

Los mercados ocultos representan un nuevo canal de distribución de drogas. Su crecimiento y su gran resiliencia frente a operaciones policiales y a fraudes dentro del propio mercado sugiere que su importancia va a aumentar en los próximos años. Hacen posible que traficantes minoristas de droga transciendan los límites geográficos, lo que aumenta potencialmente la difusión de drogas en lugares donde antes no estaban disponibles o cuya disponibilidad era limitada (Aldridge et al., 2016, p. 6).

Dentro de las prioridades operativas, Europol destaca la infiltración legítima y el cierre de comunidades en línea que fomenten la producción de materiales de pornografía infantil, sobre todo en Darknet. Asimismo considera que Darknet es un facilitador transversal del crimen. Por eso, otra de sus prioridades es combatir los sitios de comercio ilegal en la Internet Oscura. Aparte, Europol (2015, p. 15) recomienda implantar acciones que fomenten la compartición de inteligencia y los análisis tácticos, especialmente sobre esas cuestiones preferentes.

En el caso de la explotación sexual de menores, los criminales que se mueven en Darknet parecen estar más cómodos a la hora de cometer abusos y discutir sus preferencias sexuales por menores que aquellos que usan la Surface Web. Un mayor anonimato y relaciones de camaradería pueden favorecer sus impulsos sexuales, que podrían no manifestarse en ningún otro ambiente que careciera de esas características (Europol, 2015, p. 30).

Los delincuentes relacionados con la explotación sexual a menores siguen aprovechando las redes anónimas para ocultar sus actividades de los cuerpos de seguridad. Las comunidades de delincuentes evolucionan y aprenden de los errores cometidos por aquellos que han sido detenidos por la policía, lo que dificulta la infiltración. Los

usuarios de Darknets están continuamente desarrollando relaciones de confianza y comparten experiencias técnicas. Sensaciones de seguridad, reforzadas por la percepción de anonimato y por un fuerte apoyo por parte de una comunidad de ideas similares, influyen en el comportamiento de los individuos haciéndolos más propicios a cometer delitos (Europol, 2015, p. 31).

Los pagos entre criminales también son más sencillos en Dark Web. Servicios ocultos como Agora o el desaparecido Evolution están dedicados casi en exclusiva a pagos con Bitcoin, con mecanismos de gestión y funciones de fideicomiso construidas en interfaces de mercado. Actualmente, Bitcoin es clave en muchas investigaciones policiales dentro de la Unión Europea, ya que representa más del 40% de los pagos entre criminales detectados (Europol, 2015, p. 46).

La Internet Oscura favorece igualmente las comunicaciones entre delincuentes. El uso de foros en Deep Web o en Dark Web son muy comunes. Dichos foros son puntos de encuentro y de intercambio para criminales que hacen negocios y establecen relaciones con individuos de ideas afines. En julio de 2015, tuvo lugar la Operación Bugbite que logró acabar con Darkode, el foro cibercriminal en inglés más prolífico hasta la fecha. Ese foro abarcaba una amplia variedad de productos y servicios relacionados con el cibercrimen, incluyendo malware, exploits de Día Cero, hacking, robo de credenciales y de tarjetas bancarias, botnets en alquiler y ataques de denegación de servicio distribuidos (DDoS) (Europol, 2015, p. 50).

El uso de Dark Net en el tráfico de drogas ha aumentado en los últimos años, y los beneficios de ese tráfico presentan un fuerte potencial para financiar el terrorismo y los extremismos violentos. El suministro de drogas vía Internet, incluyendo mercados en línea anónimos en Dark Net, es cada vez más relevante. El potencial de Dark Net para atraer nuevos grupos de consumidores preocupa a la Oficina de las Naciones Unidas contra la Droga (UNODC), debido a que facilita el acceso a las drogas tanto en países desarrollados como en desarrollo (UNODC, 2016, pp. v y xiii).

Los cuerpos de seguridad y los sistemas de justicia penal de muchos países todavía no se encuentran capacitados para tratar eficazmente con los mercados en línea anónimos en Dark Net. Aparte de problemas prácticos, hay otras dificultades legales que deben solucionarse, como la identificación de la jurisdicción responsable y la rutina internacional de compartir información, especialmente cuando la localización física de compradores y vendedores es desconocida (UNODC, 2016, p. xv).

La compra de drogas vía Dark Net está aumentado. No solo preocupa en términos de atraer a nuevos consumidores, sino además porque los usuarios pueden evitar el contacto directo con criminales y con la policía. Los buscadores web tradicionales no permiten acceder a Dark Net. Así compradores y vendedores suelen utilizar Tor para intentar ocultar su identidad. Los productos se suelen pagar con bitcoins u otras criptomonedas y se suelen despachar vía servicios postales (UNODC, 2016, p. 24).

Según una reciente encuesta mundial, la proporción de internautas que usan Dark Net para comprar drogas ha crecido, alcanzando un 6,4% en 2014. Ese porcentaje todavía es mayor entre los nuevos consumidores de estupefacientes, con un aumento del 25% entre 2013 y 2014. Los entrevistados mencionaban varias ventajas de comprar drogas en Dark Net. Una es el propio producto, que suele ser de mayor calidad y estar más disponible. Otra es el hecho de que las interacciones del comprador sean

virtuales, lo que reduce el riesgo de seguridad personal durante las transacciones, porque evita la exposición a violencia física. A esto se añade que reduce la sensación de peligro de ser detenido por la policía. Todos estos factores ayudan a explicar por qué los compradores de drogas en Dark Net suelen estar dispuestos a pagar precios más altos y por qué esos mercados atraen a nuevos clientes. Casi un 4% de los encuestados manifestaba que nunca había consumido drogas antes de empezar a entrar en la Internet Oscura. Por otro lado, el 30% de los compradores de estupefacientes vía Dark Net señalaba haber consumido una mayor variedad de drogas que antes de empezar a aprovisionarse en esos mercados ocultos (UNODC, 2016, pp. 24-25).

El terrorismo se ha mudado a Deep Web. La Surface Web convencional se ha hecho demasiado peligrosa para los terroristas que buscan el anonimato; allí se les puede monitorizar, rastrear y localizar. Por el contrario, en Dark Web, las redes descentralizadas y anónimas ayudan a evitar arrestos y el cierre de plataformas terroristas. La tendencia reciente es que los terroristas usen Dark Web para comunicarse, conseguir financiación y almacenar información y otros materiales en línea (Weimann, 2016, p. 40).

La seguridad pública no es una misión exclusiva de la policía. Hace falta un enfoque integral con muy diversos actores implicados. Los cuerpos policiales no van a ser capaces de afrontar el problema en solitario. Las empresas, las agencias, los departamentos gubernamentales, la industria y las universidades -cualquiera que tenga experiencia en el campo de lo ciber aunque no esté relacionado con la persecución de delitos- tienen un papel relevante para mantener la seguridad pública (UK Government Office of Science, 2015, p. 57).

En su último informe sobre crimen organizado en Internet (IOCTA), Europol sugiere varias recomendaciones relacionadas con Darknets. Una de ellas es que los cuerpos de seguridad deberían recopilar proactivamente inteligencia relacionada con los servicios ocultos. Cada Estado miembro de la Unión Europea debería proporcionar inteligencia sobre estos servicios ocultos a Europol. Para ello hace falta un mayor compromiso por parte las fuerzas policiales no dedicadas específicamente al cibercrimen, porque la venta de drogas y la de armas en esos mercados de la Internet oculta representan una parte muy relevante de ese tipo de tráficos. Otra recomendación insiste en la necesidad de colaboración entre los cuerpos de seguridad, el sector privado y la universidad para explorar investigaciones relacionadas con tecnologías emergentes en Dark Web como los mercados descentralizados como OpenBazaar (Europol, 2015, p. 53).

4. DIFICULTADES DE EXPLOTACIÓN

Utilizar Deep Web como fuente de ciberinteligencia no es una tarea sencilla. Esta parte de Internet tiene una serie de peculiaridades que limitan su explotación. El gran escollo es recopilar los datos. La información no está directamente accesible como páginas web, porque suele estar detrás de formularios web.

Generalmente, los formularios web se presentan como una colección de campos de entrada, casillas de verificación, listas desplegables y otros elementos de selección, algunos de los cuales pueden ser obligatorios. Actúan como una interfaz que especifica todos los posibles patrones de acceso subyacentes en los datos, y los protege de accesos no deseados (Bienvenu, Deutch, Martinenghi, Senellart y Suchanek, 2012, p. 2).

Además, acceder a los datos de Deep Web es costoso, debido a la latencia de acceso en la red. Diversas limitaciones entorpecen el acceso a los datos, lo que todavía encarece más las consultas. Algunas fuentes solo proporcionan sus registros en lotes de tamaño fijo. Otras solo conducen a los registros superiores, en función de un ránking, dejando fuera el resto. En otros casos, solo admiten una cantidad limitada de accesos en un periodo concreto. Ciertas fuentes solo dan información incompleta, por ejemplo, presentando únicamente un subconjunto de los campos subyacentes, o bien distribuyen los datos con un nivel de granularidad diferente al que requieren otras fuentes, como meses frente a fechas completas (Bienvenu et al., 2012, p. 2).

Otro reto importante es la heterogeneidad de los datos. Conviene considerarlo a la hora de diseñar estrategias de obtención de información y de seleccionar las técnicas de Knowledge Discovery adecuadas para cada caso. En Deep Web pueden encontrarse tres tipos de contenidos:

- Datos dinámicos. Solo son accesibles a través de su interfaz de consulta. Esas interfaces pueden estar basadas en atributos de entrada y una consulta de un usuario puede involucrar valores específicos
- Contenidos sin enlazar. Los datos no están disponibles durante los análisis realizados por las arañas web tradicionales.
- Contenidos que no son texto. Diversos formatos de archivos multimedia, PDF y documentos que no son HTML (Khurana y Chandark, 2016, p. 209).

Básicamente hay tres etapas que hay que completar para poder acceder a los contenidos en Deep Web. En primer lugar, encontrar las fuentes de datos. En segundo, seleccionarlas. Por último, enviar las fuentes de datos elegidas al sistema de integración de datos.

Dependiendo de cómo sea el sistema de integración, se pueden añadir varias fuentes de datos. Sin embargo, no deberían incluirse todas dentro del sistema, por estos motivos:

- Podrían añadirse datos redundantes.
- Los datos irrelevantes podrían reducir la calidad global del sistema.
- Podrían introducirse datos de baja calidad.
- Aumentarían los costes de adquisición de datos (Khurana y Chandark, 2016, p. 210).

Suelen emplearse tres tipos de técnicas para acceder a los datos en Deep Web: Procesado de formularios y consultas a bases de datos web; correspondencia de esquema; y otras técnicas de extracción (Khurana y Chandark, 2016, p. 210).

1. Procesado de formularios y consultas a bases de datos web

Dada la enormidad de datos almacenados en la web oculta, para poder acceder a ellos hace falta rellenar y enviar formularios para conseguir la información de las bases de datos. Las arañas (*crawlers*) para Deep Web son la técnica más empleada. Se puede distinguir entre los genéricos y los verticales. Los genéricos realizan búsquedas en anchura, mientras que los verticales hacen búsquedas en profundidad concentrándose en un tema específico.

2. Correspondencia de esquema

La correspondencia de esquema (*matching schema*) es el proceso de identificar dos objetos semánticamente relacionados. En lugar de rellenar el formulario en el sitio Deep Web y luego extraer los datos para comprobar si son relevantes, se prepara un esquema de los datos requeridos. Eso reduce los costes de extracción y procesado.

3. Otras técnicas de extracción en búsquedas Deep Web.

Entre ellas figuran la minería de datos, las arañas web basadas en ontología, el clustering o la extracción visual de datos. Tienen en común que, en lugar de extraer la información completa y luego parsearla, solo capturan la sección que contiene la información relevante (Khurana y Chandark, 2016, 210, pp. 415-416).

Antes de poder extraer los datos almacenados en Deep Web es necesario establecer un conjunto de normas que determinen la información de interés (ejemplos positivos) y descarten los datos espurios (ejemplos negativos). Existen diversas propuestas para elaborar esas reglas de aprendizaje, que además deben ser adaptables, porque la web evoluciona rápidamente (Jiménez y Corchuelo, 2015, p. 140). Por ejemplo, es posible adoptar un enfoque de arriba-abajo, que empieza con la regla más general y va añadiendo iterativamente condiciones basadas en las características del catálogo hasta que la regla ya no encuentra ningún ejemplo negativo. El proceso finaliza cuando todos los ejemplos positivos coinciden. En caso contrario, el proceso continúa aprendiendo nuevas reglas. El sistema incluye mecanismos para evitar que se generen reglas demasiado complejas o excesivamente específicas. Esta propuesta de aprendizaje de reglas permite extraer información de interés desde Deep Web de forma automática, para que pueda ser procesada posteriormente por agentes de software. Para disminuir el coste de las búsquedas, se incluye una técnica que reduce los ejemplos negativos (Jiménez y Corchuelo, 2015, pp. 141 y 149).

Automatizar procesos es otro escollo complicado de superar. Uno de los primeros procesos que tiene que ser automático es la identificación de la interfaz de búsqueda en Deep Web. En un entorno de aprendizaje automático, hace falta un clasificador binario que diferencie entre interfaces buscables y no buscables. Se pueden usar varios métodos como árboles de decisión o redes de neuronas artificiales, entre otros. Sin embargo, independientemente del algoritmo de aprendizaje utilizado, suelen ser técnicas supervisadas que deben enfrentarse al problema de la escasez de datos etiquetados (Wang, Xu y Zhou, 2014, p. 635).

Por otro lado, en Deep Web es habitual que las páginas de resultados de consultas se generen dinámicamente desde las bases de datos en respuesta a las consultas enviadas por los usuarios. Extraer automáticamente datos estructurados de dichos resultados es un problema complicado, porque la estructura de los datos no está explícitamente representada (Anderson y Hong, 2013, p. 1233).

Los servicios en Deep Web presentan interdependencias, sobre todo cuando un mismo dato está disponible por varias vías. Es aconsejable tenerlo en cuenta para planificar y optimizar las consultas. Por eso, la diversificación y la eliminación de duplicados son aspectos que no deberían olvidarse (Bienvenu et al., 2012, p. 2). Así, identificar y deshacerse de los registros duplicados es otra tarea clave a la hora de preprocesar datos de Deep Web, sobre todo cuando se trata de integrarlos desde

múltiples orígenes. Las técnicas de aprendizaje automático pueden ayudar en esta operación y contribuir a reducir los costes de etiquetado. Y es que las técnicas estándar de detección de duplicados no funcionan bien en este ámbito, como, por ejemplo, escoger aleatoriamente parejas de registros o usar otras distribuciones. El objetivo final es identificar los registros duplicados de la misma o de distintas bases de datos, incluso si los registros no son idénticos (Zhao, Xin, Xian y Cui, 2014, pp. 125-127).

En muchos casos, encontrar instancias raras o atípicas (*outliers*) puede ser mucho más interesante que hallar patrones. Un valor atípico es aquel que se desvía tanto de otras observaciones que despierta la sospecha de que ha sido originado por un mecanismo distinto. Desde el punto de vista de la seguridad, hay muchos escenarios en los que resulta muy útil descubrir comportamientos que se salen de la norma. La cuestión es que los métodos habituales de minería de datos son inaplicables en Deep Web, porque se necesita conocer la distribución subyacente a los datos, algo que es impracticable en el contexto de la Internet Profunda (Xian, Zhao, Sheng, Fang, Gu, Yang y Cui, 2016, p. 1).

Entre las posibles soluciones, la más simplista, pero muy costosa, es descargar todos los registros de la base de datos subordinada y minar los atípicos con técnicas tradicionales (métricas de distancia y de densidad, o clustering, por ejemplo). La segunda alternativa es efectuar un muestreo aleatorio en la base de datos subordinada existente en Deep Web. Eso requeriría gran cantidad de muestras, lo que encarecería demasiado el proceso (Xian et al., 2016, p. 2).

Otra posibilidad consiste en desglosar la detección de valores atípicos en Deep Web en tres fases: estratificación, muestreo por vecindad y muestreo por incertidumbre. Primero se crea un esquema de estratificación a través de un árbol jerárquico que modele la relación entre los atributos de entrada y los de salida. Luego, en lugar de realizar un muestreo aleatorio por todo el estrato, se puede aplicar un esquema de muestreo por vecindad para recopilar más valores atípicos. Seguidamente, un algoritmo de muestreo por incertidumbre se ocupa de verificar las instancias dudosas para mejorar el proceso de detección (Xian et al., 2016, p. 12).

Por su parte, los cuerpos de seguridad se enfrentan a tres retos adicionales en Deep Web: el cifrado, la atribución y la fluctuación.

1. Cifrado: Todo lo que hay en Deep Web y Dark web está cifrado. Eso significa que los delincuentes son mucho más conscientes de estar vigilados y de la posibilidad de ser atrapados. El cifrado es la primera contramedida para evitar la detección.

2. Atribución: En Deep Web todavía es mucho más complicado determinar la atribución que en Surface Web. Todo sucede en dominios como los .onion (Tor). El enrutado a esos dominios tampoco está claro.

3. Fluctuación: Deep Web es un lugar muy dinámico. Un foro en línea puede estar en una dirección URL un día y otro en otra. Los esquemas de nombres y direcciones a menudo cambian. Eso significa que la información recopilada hace un par de semanas hoy deja de ser relevante. Eso tiene consecuencias a la hora de conseguir pruebas de delitos. Si se tienen en cuenta los plazos que tardan los procedimientos judiciales penales, los cuerpos de seguridad deben ser capaces de documentar rigurosamente cualquier actividad criminal en línea mediante

capturas de pantalla con sellos de tiempo para evitar que sus casos sean invalidados (Ciancaglini et al., 2015, p. 38).

5. EJEMPLOS DE USO

El uso de técnicas minería de datos y Knowledge Discovery en Deep Web y Dark Web está extendido, aunque en constante evolución. Las áreas que captan una mayor atención por parte de los investigadores son las arañas (*crawlers*) para Deep Web, los sistemas de detección y prevención de intrusiones (IDPS) y la detección de comunidades virtuales.

5.1. ARAÑAS PARA DEEP WEB

Deep Web sigue creciendo a un ritmo muy rápido. Esto aumenta el interés en desarrollar técnicas eficientes de localizar recursos. Aparte es crucial idear estrategias de rastreo en la Internet Profunda para descubrir rápidamente fuentes con contenidos relevantes. Para recolectar información en Deep Web hace falta un enfoque que proporcione una amplia cobertura pero que además mantenga una alta eficiencia de rastreo (Zhao, Zhou, Nie, Huang y Jin, 2015, pp. 1-2).

Explorar la web oculta implica dos tareas: descubrir recursos y extraer contenidos. La primera se ocupa de encontrar automáticamente sitios web que contienen interfaces con formularios de búsqueda. La segunda trata de obtener información de esos filtros filtrando los formularios mediante consultas o palabras clave relevantes (Gupta y Bhatia, 2014, p. 112).

Para completar esas tareas, una araña para Deep Web debe simular las operaciones del navegador del usuario, por ejemplo, rellenar formularios o hacer clic en el botón de aceptar (Yu, Guo, Yu, Xian y Yan, 2014, p. 5050).

En un escenario real de Deep Web, normalmente es imposible aplicar un algoritmo que cubra todos los documentos. El algoritmo todavía los desconoce. Además, el volumen de datos suele ser tan grande que ni siquiera los algoritmos de carácter aproximativo lo pueden manejar. La única opción es ejecutar un algoritmo sobre una muestra con un subconjunto de los datos (Wang, Lu y Chen, 2014, p. 199).

Los materiales en Dark Web tienen importantes implicaciones para la ciberinteligencia y la ciberseguridad. La recopilación de dichos contenidos también es relevante para estudiar diversos puntos de vista sociales y políticos presentes en esas comunidades virtuales. En concreto, los foros en Dark Web muestran una problemática faceta que está asociada con el cibercrimen, el odio y los extremismos. La naturaleza encubierta de esa parte de Internet hace que las técnicas tradicionales de rastreo web sean insuficientes para capturar tales contenidos. El sistema suele estar asistido por humanos, que se encargan de registrarse como miembros. Después entran en acción las arañas, que localizan, recopilan e indexan la información según parámetros predeterminados (Fu, Abbasi y Chen, 2010, pp. 1213-1214).

Las arañas para rastrear foros en Dark Web tienen tres dificultades de diseño. La primera es la accesibilidad; suelen requerir registrarse como miembro, a veces incluso por invitación. En segundo lugar, son multilingües. En tercer lugar, incorporan

contenidos multimedia en muy diversos formatos (fotos, vídeos y audios) que, al no ser de texto, resultan complicados de indexar (Fu, Abbasi, A. y Chen, 2010, p. 1214).

5.2. SISTEMAS DE DETECCIÓN Y PREVENCIÓN DE INTRUSIONES (IDPS)

Los sistemas de detección y prevención constituyen un área muy relevante donde aplicar minería de datos en el campo de la lucha contra el cibercrimen. Los avances en Tecnologías de Información y Comunicación (TIC) están propiciando que los delincuentes usen el ciberespacio para cometer ciberdelitos. Las ciberinfraestructuras son altamente vulnerables a intrusiones y otras amenazas. Dispositivos físicos como sensores y detectores no son suficientes para monitorizar y proteger las infraestructuras. Hacen falta sistemas de ciberdefensa flexibles, adaptables y robustos, capaces de detectar una amplia variedad de amenazas y de tomar decisiones inteligentes en tiempo real. En este contexto son de utilidad agentes semiautónomos inteligentes capaces de detectar, evaluar y responder a los ciberataques (Dilek, Çakır y Aydın, 2015, p. 21).

Diversas técnicas relacionadas con la minería de datos están ganando importancia en los sistemas de detección y prevención de intrusiones (IDPS). Es el caso de las redes de neuronas artificiales (ANN), los agentes inteligentes, los sistemas inmunes artificiales (AIS), los algoritmos genéticos o los conjuntos difusos, entre otras.

La Tabla 1 resume las ventajas que esas técnicas de minería de datos aportan a los sistemas de detección y prevención de intrusiones (IDPS).

Redes de neuronas artificiales (ANN)	Procesado de información en paralelo. Aprendizaje mediante ejemplos. Capaces de manejar complejas funciones no lineales. Resiliencia al ruido y a datos incompletos. Modelos de aprendizaje versátiles y flexibles. Intuitivos, al ser una abstracción de redes neurales biológicas.
Agentes inteligentes	Movilidad. Buena disposición para intentar completar una tarea incluso con objetivos contradictorios. Racionalidad al lograr sus objetivos. Adaptabilidad al entorno y a las preferencias del usuario. Colaboración con el usuario para comprobar inconsistencias en los datos.
Sistemas inmunes artificiales (AIS)	Estructura dinámica y robustez. Aprendizaje distribuido y en paralelo. Autoadaptable para actualizar las marcas de intrusión sin intervención humana. Respuesta selectiva y optimización de recursos. No dependiente de un único componente que puede ser fácilmente sustituido por otro.
Algoritmos genéticos	Robustez. Adaptabilidad al entorno. Optimización de soluciones a problemas computacionales complejos. Evaluación de múltiples esquemas en paralelo. Búsquedas flexibles y globales.
Conjuntos difusos	Mecanismo de razonamiento interpolativo robusto; Interoperabilidad; y Amigables para usuarios humanos.

Tabla 1. Ventajas de algunas técnicas de minería de datos para los sistemas de detección y prevención de intrusiones. Fuente: Elaboración propia a partir de Dilek, Çakır y Aydın, 2015, pp. 32-33.

Por otro lado, los sistemas actuales de detección y prevención de intrusiones (IDPS) permiten reconocer anomalías y ataques desconocidos previamente, pero también presentan importantes limitaciones (Dilek et al, 2015, p. 33):

1. La principal es construir un modelo sólido sobre lo que es un comportamiento aceptable y lo que es un ataque. Se puede producir un elevado número de falsos positivos, causados por un comportamiento atípico que realmente es normal y está autorizado.
2. Estos sistemas deben ser capaces de caracterizar patrones normales y para crear un modelo de comportamiento normal necesitan amplios conjuntos de datos de entrenamiento. Cualquier cambio en los patrones normales requieren actualizar la base de conocimiento del sistema.
3. Si el sistema clasifica incorrectamente una actividad legítima como maliciosa, el resultado puede ser un intento de parar esa actividad o cambiarla.
4. Cualquier sistema de detección, sin importar lo eficiente que sea, puede ser desactivado por los atacantes si averiguan cómo funciona.
5. En entornos heterogéneos también está la cuestión de integrar la información procedente de distintos sitios.
6. Los sistema asimismo deben ser diseñados de forma que cumplan las normas legales, los requisitos de seguridad y los acuerdos de niveles de servicio correspondientes.

Ciertos sistemas IDPS se ocupan de analizar el comportamiento de las redes. Examinan el tráfico de red para identificar amenazas que generan flujos de tráfico inusuales, como pueden ser los ataques de denegación de servicio. Se pueden utilizar sistemas de monitorización a gran escala para detectar ataques DDoS a partir de datos de tráfico en Darknet. Por ejemplo, algunos son adaptativos y emplean un modelo de aprendizaje supervisado a través de máquinas de soporte vectorial (SVM). Trabajan con los paquetes observados en Darknet; algunos son fácilmente distinguibles a partir de los números de los puertos de origen y destino, y de las banderas (*flags*), pero otros no. Para detectar los paquetes complicados, el sistema extrae características determinadas basándose en estadísticas y las clasifica usando un modelo SVM. Además, para tratar los cambios en los patrones de actividad, se aplica un aprendizaje incremental (Furutani et al., 2015, p. 382).

5.3. DETECCIÓN DE COMUNIDADES

La identificación de comunidades virtuales en Dark Web resulta de gran utilidad no solo en el crimen organizado, sino también en la lucha contra el terrorismo y los extremismos violentos. Para estudiarlas se pueden combinar técnicas de análisis de redes sociales (SNA) con minería de datos. Dark Web ofrece un inagotable potencial para lograr la coordinación, la distribución de propaganda y otras interacciones no deseadas entre grupos extremistas, terroristas y ciberdelincuentes. El reto está en identificar esas comunidades y a sus líderes.

Las comunidades virtuales en Dark Web reúnen a miembros que comparten intereses sobre determinados temas. Por eso, para comprenderlas resulta fundamental conocer cuáles son los principales intereses en cada una. A partir de ahí es posible identificar a sus miembros clave, por ejemplo, los líderes de opinión. Un miembro clave sería una persona totalmente alineada con las metas y los temas de la comunidad que produce contenidos que son muy relevantes para satisfacer los intereses del resto de los miembros. Los miembros clave pueden o no estar altamente radicalizados, pero lo que siempre sucede es que aumentan las interacciones en la comunidad gracias a sus mensajes, que producen réplicas de miembros de distintos niveles (L'Huillier, Alvarez, Ríos y Aguilera, 2010, pp. 66-67).

En una comunidad virtual hay metas diferentes asociadas con los objetivos de sus miembros. El apoyo de la comunidad en un foro en Dark Web donde reina el anonimato, la ubicuidad y la libertad de expresión es el ambiente perfecto para compartir propaganda fundamentalista y terrorista. Un método para reconocer los objetivos subyacentes de los miembros requiere identificar amenazas o cuestiones de seguridad (L'Huillier et al., 2010, p. 67).

La topología de las Darknets comparte propiedades con otros tipos de redes sociales, donde las estructuras de mundo pequeño están determinadas por las propiedades del flujo de información, y caracterizadas por un camino medio corto y por un alto coeficiente de clustering. Se pueden emplear diferentes medidas de centralidad, como el grado, la intermediación (*betweenness*) y la cercanía, para identificar a los miembros clave de una comunidad. Este análisis de redes sociales se puede completar con minería de datos de texto mediante análisis semántico latente. Generalmente se elabora un modelo de evaluación y selección que mejora la clasificación de los mensajes que contienen información sensible sobre las opiniones y sentimientos de los extremistas. Además el análisis de autoría de las tendencias del grupo debe lidiar con el problema del anonimato asociado a este tipo de comunidades virtuales (L'Huillier et al., 2010, p. 67).

6. CONCLUSIONES

La minería de datos, entendida en sentido amplio, puede ser un gran aliado en entornos fluctuantes y dinámicos como Deep Web y Dark Web. Sus técnicas que pueden ayudar a encontrar sentido a cantidades ingentes de datos. También pueden contribuir a reducir la sobrecarga informativa y cognitiva de los miembros de los cuerpos y fuerzas de seguridad y de la comunidad de la inteligencia.

En Deep Web y Dark Web se puede encontrar información valiosa sobre amenazas, vulnerabilidades y riesgos. Actualmente son fuentes muy importantes para la ciberinteligencia. Las potentes técnicas de minería de datos permiten convertir datos en conocimiento. Por ejemplo, sirven para desvelar patrones e identificar tendencias.

Es esencial tener claros los objetivos y la estrategia desde el principio. Así será posible seleccionar las técnicas de minería de datos y de Knowledge Discovery adecuadas para cada caso. A menudo va a ser necesario adaptarlas a las peculiaridades del campo de la seguridad. Tampoco hay que olvidar la importancia de interpretar y evaluar los resultados antes de presentarlos a los decisores. Además, el contexto lo cambia todo. Algo que funciona en un contexto y en un momento determinados puede no hacerlo en otros.

La minería de datos no está libre de limitaciones. Una de ellas es la buena calidad de los datos, que no es fácil de lograr en Deep Web, como antes se ha reseñado, por dificultades técnicas y de costes. Otra limitación está relacionada con los falsos positivos y los falsos negativos, esto es, la precisión y la sensibilidad de los modelos generados. En tercer lugar, está la cuestión de la rareza, en el sentido de poca frecuencia. Los hechos delictivos son eventos poco frecuentes, lo que hace poco fiable la extrapolación de los modelos.

En definitiva, la minería de datos y el Knowledge Discovery son útiles herramientas que conviene manejar con sabiduría y prudencia, siendo conscientes de sus limitaciones.

AGRADECIMIENTOS

A Ramón Fuentes por leer el borrador de este artículo.

REFERENCIAS BIBLIOGRÁFICAS

Aldridge, J. y Décary-Hétu, D. (2016). Hidden wholesale: The drug diffusing capacity of online drug cryptomarkets. *International Journal of Drug Policy* (en prensa).

Anderson, N. y Hong, J. (2013). Visually Extracting Data Records from the Deep Web. *WWW '13 Companion Proceedings of the 22nd International Conference on World Wide Web*, 1233-1238.

Bienvenu, M., Deutch, D., Martinenghi, D., Senellart, P. y Suchanek, F. (2012). Dealing with the Deep Web and all its Quirks. En M. Brambilla, S. Ceri, T. Furche, & G. Gottlob (Eds.), *VLDS 2012: Very Large Data Search* (pp. 21-24). Aachen: CEUR.

Bergman, M. (2001). *The Deep Web: Surfacing Hidden Value*. BrightPlanet. Disponible en http://brightplanet.com/wp-content/uploads/2012/03/12550176481-deep-webwhitepaper1.pdf

Chen, H. (2012). *Dark Web: Exploring and Data Mining the Dark Side of the Web*. Nueva York: Springer.

Ciancaglini, V., Balduzzi, M., McArdle, R. y Rösler, M. (2015). *Below the Surface: Exploring the Deep Web*. Trend Micro. Disponible en https://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp_below_the_surface.pdf

Dilek, S., Çakır, H. y Aydın, M. (2015). Applications of Artificial Intelligence Techniques to Combating Cyber Crimes: A Review. *International Journal of Artificial Intelligence & Applications (IJAIA), 6*(1), enero 2015, 21-39.

Europol. (2015). *The Internet Organised Crime Threat Assessment (IOCTA) 2015*. La Haya: Europol.

Fachkha, C. y Debbabi, M. (2016). Darknet as a Source of Cyber Intelligence: Survey, Taxonomy, and Characterization. *IEEE Communications Surveys & Tutorials, 18*(2), 1197-1227.

Fu, T., Abbasi, A. y Chen, H. (2010). A Focused Crawler for Dark Web Forums. *Journal of the American Society for Information Science and Technology, 61*(6), 1213-1231.

Furutani, N., Kitazono, J., Ozawa, S., Ban, T., Nakazato, J. y Shimamura, J. (2015). En Arik, Sabri, Huang, Tingwen, Lai, Weng Kin y Liu, Qingshan (Eds.), *Neural Information Processing, 22nd International Conference, ICONIP 2015, Istanbul, Turkey, November 9–12, 2015 Proceedings, Part IV* (pp. 376-383). Cham: Springer.

Gobierno de España. (2013). *Estrategia de Ciberseguridad Nacional 2013*.

Gobierno de España. (2016). *Informe Anual de Seguridad Nacional 2015*.

Goodman, M. (2015). *Future Crimes: A Journey to the Dark Side of Technology - and How to Survive it*. Londres: Transworld Publishers.

Gupta, S. y Bhatia, K. K. (2014). A Comparative Study of Hidden Web Crawlers. *International Journal of Computer Trends and Technology, 12*(3), 66, 111-118.

Han, J., Kamber, M. y Pei, J. (2012). *Data Mining: Concepts and Techniques*. Waltham: Elsevier.

Hardy, R. A. y Norgaard, J. R. (2015, 4 de noviembre). Reputation in the Internet black market: an empirical and theoretical analysis of the Deep Web. *Journal of Institutional Economics*, 1-25. doi: 10.1017/S1744137415000454

Hawkins, B. (2016). *Under The Ocean of the Internet - The Deep Web*. SANS Institute Reading Room. Disponible en https://www.sans.org/reading-room/whitepapers/covert/ocean-internet-deep-web_37012

Jiménez, P. y Corchuelo, R. (2015). On Extracting Information from Semi-structured Deep Web Documents. En Abramowicz, W. (Ed.), *Business Information Systems, 18th International Conference, BIS 2015, Poznań, Poland, June 24-26, 2015, Proceedings* (pp. 140-151). Cham: Springer.

Khurana, K. y Chandak, M. B. (2016). Survey of Techniques for Deep Web Source Selection and Surfacing the Hidden Web Content. *International Journal of Advanced Computer Science and Applications, 7*(5), 409-418.

L'Huillier, G., Alvarez, H., Ríos, S. A. y Aguilera, F. (2010). Topic-Based Social Network Analysis for Virtual Communities of Interests in the Dark Web. *SIGKDD Explorations, 12*(2), 66-73.

Moore, D. y Rid, T. (2016) Cryptopolitik and the Darknet. *Survival, 58*(1), 7-38.

Nakao, K. (2016). IoTSecurity issues related to the future Networked Car. *Symposium on The Future Networked Car, Geneva, Switzerland, 3 de marzo de 2016*. Disponible en https://www.itu.int/en/fnc/2016/Documents/Presentations/Koji-Nakao.pdf

Pederson, S. (2013, marzo). *Understanding the Deep Web in 10 Minutes*. BrightPlanet. Disponible en http://bigdata2.brightplanet.com/whitepaper-understanding-the-deep-web-in-10-minutes

UK Government Office of Science. (2015). *Annual Report of the Government Chief Scientific Adviser 2015: Forensic Science and Beyond: Authenticity, Provenance and Assurance. Evidence and Case Studies*.

Soska, K. y Christin, N. (2015). Measuring the Longitudinal Evolution of the Online Anonymous Marketplace Ecosystem. *Proceedings of the 24th USENIX Security*

Symposium, August 12–14, 2015, Washington, D.C, 33-48.

United Nations Office on Drugs and Crime (UNODC). (2016). *World Drug Report 2016*.

Wang, H., Xu, Q. y Zhou, L. (2014). Deep Web Search Interface Identification: A Semi-Supervised Ensemble Approach. *Information, 5*, 634-651.

Wang, Y., Lu, J. y Chen, J. (2014). TS-IDS Algorithm for Query Selection in the Deep Web Crawling. En Chen, L., Jia, Y., Sellis, T. y Liu, G. (Eds.), *Web Technologies and Applications, 16th Asia-PacificWeb Conference, APWeb 2014, Changsha, China, September 5-7, 2014 Proceedings* (pp. 189-200). Cham: Springer.

Weimann, G. (2016). Terrorist Migration to the Dark Web. *Perspectives on Terrorism, 10*(3), 40-44.

Xian, X., Zhao, P., Sheng, V. S., Fang, L., Gu, C., Yang, Y. y Cui, Z. (2016). Stratification-Based Outlier Detection over the Deep Web. *Computational Intelligence and Neuroscience, 2016*, 1-13.

Yu, H., Guo, J., Yu, Z., Xian, Y. y Yan, X. (2014). A Novel Method for Extracting Entity Data from Deep Web Precisely. *26th Chinese Control and Decision Conference (CCDC),* 5049-5053.

Zhao, F., Zhou, J., Nie, C., Huang, H. y Jin, H. (2015). SmartCrawler: A Two-stage Crawler for Efficiently Harvesting Deep-Web Interfaces. *IEEE Transactions on Services Computing* (en prensa).

Zhao, P., Xin, J., Xian, X. y Cui, Z. (2014). Active Learning for Duplicate Record Identification in Deep Web. En Wen, Z, y Li, T. (Eds.), *Foundations of Intelligent Systems, Advances in Intelligent Systems and Computing 277* (pp. 125-134). Berlín: Springer.

Fecha de recepción: 21/09/2016. Fecha de aceptación: 20/12/2016

LA UTILIZACIÓN TERRORISTA DE LA TÁCTICA DE NEGACIÓN DE ÁREA

JUAN PABLO SOMIEDO GARCÍA

ANALISTA Y PROFESOR DEL CURSO DE EXPERTO EN ANÁLISIS DE INTELIGENCIA DE LA UAM. (ÁREA DE ESTUDIOS ESTRATEGICOS E INTELIGENCIA)

RESUMEN

Este trabajo se inscribe dentro del campo de las denominadas TTPs, acrónimo en inglés para designar las tácticas, técnicas y procedimientos terroristas. Se describe la táctica de negación de área y los medios utilizados por los terroristas para implementarla. De igual forma se analizan dos ejemplos históricos de su uso por parte de la banda terrorista ETA en España y de Sendero Luminoso en Perú.

Palabras clave: Terrorismo, Tácticas, Negación de Área, ETA, Sendero Luminoso

ABSTRACT

This work falls within the field of so-called TTPs, an acronym in English for “terrorist tactics, techniques and procedures”. It describes the tactic of denial area as well as the means used by terrorists in order to implement it. Furthermore, two historical examples of its use by the terrorist group ETA in Spain and Sendero Luminoso in Peru are analyzed.

Key words: Terrorism, Tactics, Denial Area, ETA, Sendero Luminoso

“Un ejército pierde si no gana, una guerrilla gana si no pierde”

Henry Kissinger

1. INTRODUCCIÓN

Es un hecho que tanto la naturaleza de los conflictos como los problemas a los que se enfrentan las Fuerzas y Cuerpos de Seguridad del Estado para afrontarlos han variado sustancialmente en el fondo y en la forma durante los últimos 50 años. Y la evolución de las diferentes tácticas para hacerles frente ha ido a caballo de esta realidad cada vez más correosa y difusa. Atrás queda la época de los conflictos simétricos interestatales donde dos bandos perfectamente diferenciados y distinguibles luchaban en frentes claramente definidos. Hoy en día la mayoría de los conflictos son intra-estatales, es decir, tienen lugar dentro del propio estado, son de carácter asimétrico y sus actores no estatales no siempre están claramente definidos ni son estables en el tiempo.

Hay muchas amenazas que pueden obstaculizar e incluso minar el correcto funcionamiento de un Estado y la sensación de seguridad de los ciudadanos y, como ya sabemos, la seguridad es una de las claves para el desarrollo económico de un país o un Estado. Kofi Annan, antiguo secretario general de la ONU, supo expresar este binomio virtuoso

cuando afirmó: “no tendremos desarrollo sin seguridad ni seguridad sin desarrollo”. Entre las amenazas más visibles podemos distinguir el narcotráfico, el crimen organizado, la ciberdelincuencia, diferentes tipos de insurgencia y el terrorismo, entre otros.

El espacio y el tiempo siempre han sido dos factores fundamentales en cualquier conflicto y, de esta forma, se han ido elaborando tácticas ofensivas y defensivas cuya meta siempre es alcanzar los objetivos previstos basándose en ambos factores. La táctica de negación de área que estudiamos en este trabajo se basa fundamentalmente en el primer factor, esto es, el factor espacio y se ha ganado sobradamente un hueco dentro del amplio abanico de las denominadas TTP´s (Terrorist Tactics, Techniques and Procedures).

La negación de área es un término utilizado en inteligencia que, de forma básica, describe un entorno operativo muy hostil con fuerte vigilancia. El Departamento de Defensa de los Estados Unidos define la negación de área como “una zona bajo el control del enemigo en las que las fuerzas aliadas no pueden esperar operar con éxito debido a las limitaciones operativas”. Pero aplicado a la lucha contraterrorista, como veremos, el término adopta una mayor complejidad debido a los diferentes medios que los terroristas utilizan para conseguirla.

La táctica de negación de área conocida por su acrónimo A2/AD hace referencia a los diferentes mecanismos militares, políticos, diplomáticos, económicos y geográficos que impiden a un enemigo movilizar fuerzas en un determinado teatro de operaciones, imposibilitando así su capacidad operativa en dicho escenario.

La preocupación por el acceso al área operativa no es ni mucho menos algo novedoso, pero sí ha experimentado modificaciones en las últimas décadas.

Así, por ejemplo, en 1988, con la Guerra Fría a punto de terminar, el Ejército de EE.UU. tenía el equivalente a cinco divisiones en el oeste de Alemania junto con aviones de combate en puntos de Europa. Por entonces, el desafío se caracterizaba principalmente en los esfuerzos del enemigo por intentar interferir en la llegada de refuerzos para las tropas que ya estaban en el área de operaciones antes del inicio de las hostilidades.

En cambio, en la Guerra del Golfo de 1991, el ejército de EE.UU tuvo que proyectar poder en regiones donde previamente no había un posicionamiento previo de personal y equipo. Los adversarios se han dado cuenta de este hecho y han comenzado a planificar operaciones e implementar capacidades para amenazar y frustrar las operaciones de llegada al territorio.

La negación de área puede basarse en aspectos de origen geográfico, militar o diplomático. El ejemplo clásico del empleo de la táctica A2/AD fue la batalla de las Termópilas. Las ciudades-Estado griegas, lideradas por el rey Leónidas I y sus 300 espartanos, aglutinaron una fuerza defensiva de 7000 hombres. Los historiadores modernos creen que los persas contaban con un total de 70.000 efectivos. Finalmente los persas ganaron la batalla pero los griegos fueron capaces de detener al ejército de Jerjes, ganando un tiempo precioso y causándole bajas cruciales.

Pero si dejamos a un lado el elemento geográfico, del que es un claro exponente el ejemplo histórico que acabamos de mencionar, la táctica de negación de área también puede basarse en cuestiones diplomáticas con otros Estados como sucedió cuando la banda terrorista ETA (Acrónimo de Euskadi Ta Askatasuna) buscaba refugio en territorio francés.

Otro ejemplo diferente pero con la misma base fue el caso de los albano-kosovares en la guerra de Kosovo, que llevaron a cabo sus operaciones de información más exitosas contra el ejército serbio a través de una diáspora activa en Suiza.

La utilización de un determinado armamento militar como las minas antipersona[1] también puede ser una forma de implementar esta táctica. Otros ejemplos los constituyen los submarinos rusos de cuarta generación, herramientas bélicas destinas a prevenir la intervención de la OTAN y de los EE.UU. en el este de Europa, o los mísiles balísticos antibuque de China DF-21D[2], cuyo objetivo es disuadir a EE.UU. de una hipotética intervención militar en la zona.

A continuación examinaremos algunos de los medios utilizados por los terroristas para implementar esta táctica basándonos en dos casos históricos como son el de la banda terrorista ETA en España y el de Sendero Luminoso en Perú.

2. EL CASO DE LA BANDA TERRORISTA ETA: LA TÁCTICA DE NEGACIÓN DE ÁREA MEDIANTE MEDIOS POLÍTICOS

Desde prácticamente los orígenes de su actividad, la banda terrorista ETA comprendió que el territorio francés podría ser un elemento clave en su estrategia no solo para escapar de la presión y el control de las fuerzas y cuerpos de seguridad del Estado y de los servicios de inteligencia en España, sino para darle al conflicto un halo de resistencia heroica contra la dictadura que conectaba directamente en el imaginario popular, todavía con las imágenes frescas y el recuerdo de la Guerra Civil, con las peripecias vividas por los maquis[3].

El "santuario francés" pronto se convirtió en un lugar donde los terroristas se sentían seguros y podian moverse con más facilidad y organizar el entramado logístico y militar e incluso económico de la banda, que sirvió para asesinar a casi 1.000 personas en España.

El gobierno francés había conferido a los miembros de la banda terrorista ETA el estatuto de refugiado político[4] con sus derechos, algo que fue un verdadero caballo

1 La moderna mina anti-persona es una evolución del antiguo abrojo, que consistía en dos o más espinas afiladas dispuestas de tal forma que las espinas siempre apuntaban hacia arriba. Uno de los primeros usos de los que se tiene noticia en un campo de batalla fue en el año 331 a.C, cuando Darío III desplegó estas armas contra Alejandro Magno en la batalla de Gaugamela.

2 El DF-21D es un misil balístico antibuque de alcance medio con capacidad de atacar una nave en movimiento en alta mar. El misil es capaz de alcanzar una velocidad hipersónica de hasta 12 Mach, lo que hace extremadamente difícil la posibilidad de derribarlo. Al mismo tiempo, el arma es un sistema móvil, por lo que sería casi imposible localizarlo antes del lanzamiento.

3 El vocablo "maquis" tuvo sus orígenes durante la II Guerra Mundial como designación de los grupos de guerrilleros que formaban parte de la resistencia francesa contra las fuerzas del Régimen de Vichy y de la Wehrmacht del Tercer Reich. En el País Vasco no fue hasta 1944 cuando el PCE (Partido Comunista Español) decidió poner en marcha la guerra de guerrillas tras el fracaso de la invasión convencional del Valle de Arán bautizada con el nombre de Operación Reconquista de España. Para ello, desde noviembre de 1944 a junio del 45 más de 40 maquis veteranos pasaron de Francia a Guipúzcoa, Vizcaya y Álava. El epilogo a los maquis en el País Vasco se escribió el 8 de agosto de 1961, cuando un grupo de 14 guerrilleros mandados por Valentín González "El Campesino", tuvo un encuentro con la Guardia Civil en Irati (Navarra).

4 Es de sobra conocida la anécdota vivida por Marcelino Oreja, ministro de asuntos exteriores del Gobierno de UCD, cuando visitó a su homólogo francés Jean Francois Poncet y puso ante sus ojos un listado de 127 presuntos etarras que vivían en territorio galo gracias al estatuto de refugiado político o al permiso de residencia.

de batalla para el gobierno español durante los primeros años de la transición. Esta situación se prolongó en el tiempo hasta el 23 de Septiembre de 1984, cuando Francia, por primera vez, extraditó a España a tres miembros de ETA y deportó a Togo a otros cuatro. Este hecho puso fin a casi 30 años de impunidad y de total libertad de movimientos de la banda en territorio galo[5]. Pero no fue hasta principios de los años 90 cuando los agentes españoles pudieron empezar a trabajar en Francia previa desarticulación de los GAL (Grupos Antiterroristas de Liberación).

La banda terrorista ETA supo utilizar el factor político para crear una táctica de negación de área que impedía al gobierno español y a las fuerzas y cuerpos de seguridad españoles sus movimientos en territorio galo mientras que servía de base operativa a la banda para planificar logística y operativamente los atentados y también le permitía financiarse a través del llamado "impuesto revolucionario" que imponía a empresarios y profesionales del país vasco bajo amenazas de asesinato, secuestro o daños contra sus propiedades.

De igual forma le sirvió para continuar creciendo en número de miembros mediante el aparato de captación y reclutamiento ("endalahar"). Cabe recordar aquí que el comando Argala, creado en 1978 por el dirigente de ETA Domingo Iturbe Abasolo "Txomin", estaba integrado exclusivamente por ciudadanos franceses (hecho excepcional en la historia de ETA). Era un grupo secreto dentro de la propia banda y operaba fuera de las normas de esta. Ser franceses y no estar fichados permitía a los terroristas llevar una doble vida sin levantar sospechas. Cuando un objetivo era marcado se trasladaban a España y se alojaban en hoteles de tres y cuatro estrellas utilizando documentación falsa, cometían el atentado y después regresaban tranquilamente de nuevo a su vida normal en Francia. Se estima que este comando, desde su creación en 1978 hasta su desarticulación en abril de 1990, es el responsable de 41 asesinatos. (Sanchez, 2016, p.35)

No obstante, su libertad de movimientos en Francia también permitió a ETA crear canales de comunicación fluida con otros terroristas, como por ejemplo el IRA (Irish Republican Army), e intercambiar información sobre tácticas y procedimientos, favoreciendo y fortaleciendo así su ciclo de aprendizaje. También es sabido que Gadafi prestó ayuda a ETA con dinero, armas y entrenamiento[6].

Además dicha libertad de movimientos no era exclusiva del territorio galo, sino que otros países europeos como Bélgica siguieron el mismo patrón y consideraban a los terroristas "perseguidos políticos". Caso contrario fue el de la nación vecina de Portugal que, desde prácticamente los primeros pasos de la banda, se mostró dispuesta a la colaboración con el gobierno español.

Como ha sucedido en otras ocasiones (algunas muy recientes), los servicios de inteligencia estratégica de algunos países vecinos vieron en la instrumentalización de la banda terrorista un poderoso mecanismo diplomático que permitía a sus respectivos gobiernos una posición ventajosa en cualesquiera tipo de negociaciones a nivel

5 ETA fue fundada en el año 1958.

6 El lector interesado puede profundizar en este aspecto consultando otro artículo del autor para el Instituto Español de Estudios Estratégicos que lleva por título: "La estructura y la organización de los grupos terroristas bajo la óptica del aprendizaje organizacional" y que figura en el apartado bibliográfico de este trabajo.

internacional. Era un as en la manga que podía ser utilizado en cualquier momento bien como excusa o bien como activo negociador.

Si bien puede considerarse que ETA ha sido finalmente doblegada[7] no es menos cierto que en su oscura existencia tiene el haber sido capaz de desestabilizar puntualmente, al menos en dos ocasiones, al Estado español y de haberlo intentando otras tantas. La primera de ellas fue en el atentado de Carrero Blanco, que hirió de muerte a la dictadura de Francisco Franco, y la segunda fue durante los sucesos acaecidos durante la creación y actuación de los Grupos Antiterroristas de Liberación (GAL)[8], con Felipe González en la presidencia. No obstante, fracasaron en el intento de asesinato del rey de España en Palma de Mallorca en 1995.

Por otro lado, debemos ser cautelosos porque la victoria sobre la banda terrorista no ha sido completa. Sus ideas independentistas aún perviven en un sector importante del pueblo vasco[9] y, a día de hoy, ningún analista se atreve a afirmar la imposibilidad del nacimiento de otro tipo de organizaciones de carácter político a partir de los rescoldos de ETA que finalmente opten por la vía del terrorismo.

Hay que tener muy presente dónde y cómo nació ETA porque ese nacimiento explica por qué muchos ciudadanos vascos creían en la legitimidad de su lucha armada[10]. La dictadura de Francisco Franco generó el caldo de cultivo para atizar la férrea resistencia de los vascos. Se les prohibió su lengua, su cultura y sus intelectuales fueron perseguidos. El clero católico en general y el vasco en particular era constantemente monitorizado por la dictadura, muchos curas sufrieron la censura en sus homilías y algunos acabaron en la famosa prisión concordataria de Zamora, que era un pabellón de la antigua prisión provincial habilitado especialmente para tal fin, acusados de ser republicanos o rojos.

En 1960, 339 sacerdotes vascos enviaron a la Sección Segunda de la Secretaría de Estado del Vaticano un escrito en el que denunciaban las detenciones, torturas y censura del régimen franquista. Este texto, en el que también se reclamaba “la defensa de los derechos del pueblo vasco y su lengua” causó verdadera impresión en la Secretaría de Estado.

Ante tal situación, la maquinaria de la diplomacia vaticana se puso en marcha. El nuncio Luigi Dadaglio, junto con los cardenales Tarancón (su mano derecha el jesuita Martín Patino),Tabera y Bueno Monreal hicieron posible, siguiendo las precisas instrucciones de Roma, que la Conferencia Episcopal Española cambiara de rumbo entre los años 1967 y 1970 y apostara decididamente por la separación Iglesia-Estado, lo

7 Con la reciente detención en Ascain de Mikel Irastorza, jefe del aparato logístico, a la banda apenas le quedarían media docena de efectivos dispersos por Francia y algunos veteranos refugiados en Venezuela y Cuba.

8 Los Grupos Antiterroristas de Liberación (GAL) fueron agrupaciones parapoliciales que practicaron lo que se ha denominado terrorismo de Estado o “guerra sucia” contra la banda terrorista ETA. Estuvieron activos entre 1983 y 1987 durante el gobierno de Felipe González y actuaban principalmente en el País vasco-francés.

9 La reciente agresión a dos guardias civiles junto con sus parejas en Alsasua (Navarra) es una violenta demostración de este hecho.

10 Conviene recordar que las ideas políticas primigenias de ETA se gestaron en un Seminario de la mano de las juventudes católicas del PNV y que la mayoría del clero y la jerarquía católica vasca apoyaron las actuaciones de la banda terrorista aún en los tiempos más sangrientos.

que minaba el régimen en su legitimación moral. La Conferencia Episcopal se opondría a la firma de un nuevo concordato en 1974, poniendo las bases de su legitimación moral de cara a la futura transición hacia la democracia.

Pero, una vez acabada la dictadura, el brazo armado de ETA se impuso en la organización y lo que había comenzado como una lucha contra la dictadura, sazonada de ciertos principios nacionalistas de Sabino Arana, acabó siendo un grupo terrorista que no dudó en asesinar civiles inocentes. Buena parte del clero vasco simpatizó y colaboró con la banda terrorista, pero esta vez ya sin el beneplácito ni de Roma ni de la Conferencia Episcopal a la que, dicho sea de paso, provocaron no pocos quebraderos de cabeza las posturas antagónicas de los obispos Setién o Uriarte.

Las causas primigenias del nacimiento de la banda terrorista ETA, los apoyos conseguidos durante la dictadura y su posterior deriva e instrumentalización independentista debería hacernos comprender hasta qué punto debemos ser cautelosos. Un grupo terrorista no nace de la nada y suele tener siempre compañeros de viaje y apoyos que, a su vez, instrumentalizan sus acciones políticamente.

Corresponde a los servicios de inteligencia y a los cuerpos y fuerzas de seguridad del Estado vigilar y neutralizar cualesquiera nuevos intentos de nacimiento de grupos armados que atenten contra la seguridad de los ciudadanos, toda vez que las exigencias que estos grupos abanderan no tienen cabida, al menos por el momento, en la Constitución española.

3. EL CASO DE SENDERO LUMINOSO: LA NEGACIÓN DE ÁREA BASADA EN ELEMENTOS GEOGRÁFICOS Y MILITARES

El caso del grupo terrorista Sendero Luminoso en el Perú, aun compartiendo la misma táctica, es diferente al de la banda terrorista ETA, pues se vale de otros medios. En este caso, la geografía y el uso sistemático de determinados elementos militares hicieron de la selva de Perú un territorio difícil al acceso y control por parte de las Fuerzas Armadas peruanas. Así, la selva de Perú se convirtió en un refugio desde el que Sendero Luminoso planificaba los atentados en la misma Lima capital. Los coches bomba, los explosivos en locales y el asesinato de policías y magistrados eran el pan de cada día que soportaba la aterrada población de Lima. Con esta ola de terror, la intención del grupo terrorista era clara, esto es, atacar el centro de gravedad del enemigo o en un lenguaje menos militar acabar con la voluntad de lucha del atemorizado pueblo peruano. Su estrategia se basaba en controlar la zona rural, donde frecuentemente reclutaban efectivos a la fuerza, para, desde allí, presionar a las ciudades. Esta estrategia tenía su origen en las ideas de Mao, que aseveraba que la forma que la conquista de poder tomaría en los países denominados semifeudales era la de “una guerra popular prolongada del campo a la ciudad”.

No olvidemos que el grupo terrorista Sendero Luminoso tuvo su origen a finales de los años 60, aunque la lucha armada comenzó en 1980. En esa época los instrumentos con los que contaba la inteligencia militar peruana no eran los actuales. La interceptación de comunicaciones era dificultosa y estaba en un estadio muy precario, la inteligencia de imágenes carecía de la ayuda de los modernos satélites y

la inteligencia humana[11] (mucho más arriesgada) apenas lograba dar frutos. Todo ello hacía que las fuerzas armadas del Perú estuvieran prácticamente ciegas y sordas y tuvieran enormes dificultades para obtener inteligencia en tiempo y forma adecuados.

Sendero Luminoso aplicaba la táctica de negación de área sobre todo a las zonas cocaleras porque el narcotráfico siempre fue una de las fuentes de financiación del grupo terrorista junto con los secuestros. Sendero Luminoso se autoproclamó defensor de los "cultivadores de la planta de coca" y se comprometió a cuidar de que estos no fueran arrestados por el gobierno, cobrándoles, eso sí, un impuesto revolucionario que equivalía a la quinta parte de la producción. También vigilaban los cargamentos de pasta de coca provenientes del Huallaga. Se estima que los ingresos obtenidos por esta actividad oscilaron entre los 20 y los 100 millones de dólares anuales, dependiendo del año.

Sendero Luminoso mostró una gran habilidad para reproducir en la selva peruana las técnicas utilizadas por el Vietcong en la guerra de Vietnam. Así implementaron una red de túneles planificados estratégicamente para poder trasladarse rápidamente hacia posiciones enemigas antes de que estas recibieran refuerzos o suministros, hicieron uso de trampas explosivas que, además de causar bajas, retrasaban el avance de las fuerzas enemigas, que perdían así la posibilidad de realizar ataques sorpresa, y utilizaron sistemáticamente ametralladoras antiaéreas y cohetes que eran un verdadero temor para los helicópteros (recordemos que en aquella época los helicópteros carecían de los dispositivos de contramedidas actuales). De hecho consiguieron derribar a más de un helicóptero M17 de transporte de tropas.

A esto había que añadir que, una vez llegados al teatro de operaciones, los militares vivían sin apenas comodidades y en muchos casos en condiciones mucho más penosas que los terroristas, que tenían bases bien asentadas y organizadas y podían desplazarse fácilmente de un lugar a otro.

Pero como afirmábamos en la introducción de este trabajo, el binomio espacio-tiempo siempre ha conformado dos factores fundamentales en cualquier conflicto y Sendero Luminoso, además de sacar partido del espacio, hizo lo propio con el tiempo. De hecho, Sendero Luminoso siempre se declaró como un grupo maoísta y precisamente si algo de creativo tiene Mao Tse-Tung como teórico de la guerra de guerrillas es el hallazgo de que un proceder lento, una desaceleración del curso de los acontecimientos, brinda la oportunidad de oponer con éxito una resistencia armada a un enemigo que es muy superior en hombres y recursos. Este hecho se notó mucho en los comienzos del conflicto armado, cuando Sendero Luminoso llevaba la iniciativa con rapidez y el ejército y las fuerzas de seguridad del Estado reaccionaban de forma muy lenta y tardía.

Una comprensión simple de la táctica A2/AD nos hace entender por qué motivo los políticos y los ciudadanos del país se quejaban continuamente de que la estrategia implementada para combatir al grupo terrorista no era la más adecuada ni parecía estar dando frutos. Dejando a un lado las dificultades de la inteligencia militar para

11 Aunque al principio la inteligencia humana se mostró claramente ineficaz, fue paulatinamente mejorando. Una muestra de esa mejora fue la captura de Óscar Ramírez Durand (Feliciano) en julio de 1999 y la del último líder histórico de Sendero Luminoso, Florindo Flores Hala (Artemio), en 2012. Artemio fue capturado con ayuda de miembros de su propia columna que previamente habían sido captados por la DIRANDRO (Antidrogas) mediante el ofrecimiento de una recompensa económica facilitada por el gobierno de EE.UU. (Antezana, 2012).

conseguir inteligencia actual[12] en tiempo y forma adecuados se pretendió combatir al grupo terrorista en dos líneas paralelas: primero bajo una perspectiva exclusivamente táctica y militar, basada en las operaciones por sorpresa y en la concentración de potencia fuego y efectivos sobre determinados objetivos, y segundo utilizando el "kingpin strategy". A continuación examinaremos estas dos líneas de acción.

La lógica subyacente detrás de la estrategia del líder o "kingpin strategy"[13], que supone que la eliminación o captura de este debe, al menos a corto plazo, dificultar el funcionamiento operativo y estratégico del grupo terrorista (Somiedo, 2015, p.19). En este apartado las fuerzas gubernamentales hicieron bien su trabajo y ya en 1992 el Grupo Especial de Inteligencia (GEIN) logró la captura y detención del líder primer histórico del movimiento, Abimael Guzmán, junto con su esposa Elena Iparraguirre y varios cabecillas de la organización. En 1999 capturaron a Feliciano. En 2012 hicieron lo propio con el histórico líder Florindo Flores Hala, más conocido por su pseudónimo de Artemio, gracias, entre otras cosas, a que un miembro de su propia columna, previamente captado por la DIRANDRO mediante el pago de una recompensa económica ofrecida por el gobierno de EE.UU., le disparó una descarga de perdigones que le hirieron en varias partes del cuerpo y a la colaboración de los hermanos Quispe Palomino, que hoy hacen las veces de mercenarios a sueldo para los narcotraficantes en la zona del VRAE. En 2013 caían Alejandro Borda Casafranca ("Alipio") y Marco Antonio Quispe Palomino ("Gabriel").

Los resultados obtenidos con la implementación de esta estrategia vienen a corroborar los análisis realizados por Jenna Jordan de que los grupos con ideología política radical son más propensos a cesar su actividad con la implementación de la kingpin strategy que los que están basados en motivaciones religiosas (Jordan, 2009, p.734).

La kingpin strategy obtuvo resultados en dos líneas diferentes. Por un lado logró dislocar a la organización terrorista y frenar su crecimiento y, por otro, no menos importante, logró que aparecieran desavenencias y luchas de poder en el interior de la propia banda que finalmente se dividió en dos facciones diferentes: por una parte la facción histórica de Sendero Luminoso que tiene como referente a Abimael Guzmán y que era partidaria de iniciar negociaciones de paz con el gobierno y, por otro, el denominado "Sendero Rojo", al mando de Feliciano. A esta facción pertenecen los últimos rescoldos de la organización liderados por los hermanos Quispe Palomino, que más que un grupo terrorista con objetivos políticos son una banda armada al servicio del narcotráfico del VRAE. La inteligencia militar supo sacar provecho de estas luchas de poder interna captando colaboradores e informadores que jugarían un papel decisivo en el conflicto.

La segunda línea de acción implementada por el gobierno fue la táctica y militar. La historia proporciona varios ejemplos de que combatir la insurgencia desde un enfoque fundamentalmente táctico es un claro error. Este enfoque tiene poco efecto a largo

12 La inteligencia actual tiene dos funciones básicas: mantener al día la inteligencia básica con datos nuevos (para lo que adopta a forma de boletines periódicos, generalmente diarios, sobre cuestiones específicas de interés habitual) y responder de modo rápido y preciso a una petición de información sobre una cuestión de actualidad o hechos concretos que se deben conocer para la toma de una decisión, con los datos disponibles o mediante un proceso de búsqueda "ad hoc" con los recursos que se poseen.

13 Para un conocimiento más exhaustivo de esta estrategia recomiendo al lector la lectura del trabajo "La estructura y la organización de los grupos terroristas bajo la óptica del aprendizaje organizacional" que aparece en el apartado bibliográfico de este trabajo.

plazo porque las fuerzas no crean una presencia permanente ni interrelacionan con la población. En el caso objeto de estudio, la estrategia de Sendero Luminoso siempre fue dominar las zonas rurales para desde allí presionar a las ciudades. Reclutaban a sus efectivos, muchos de ellos obligados por la fuerza, entre la población campesina de las zonas rurales y alejadas de los focos de población.

Fue una lección que terminaron por aprender las fuerzas coloniales francesas en África a finales del siglo XIX. Introdujeron el concepto de ocupación progresiva y penetración económica combinadas con el uso de la fuerza militar. Así a la lucha en el terreno militar unieron instrumentos políticos y económicos para favorecer un cambio permanente de la situación.

El ejército estadounidense utilizó un enfoque similar a principios del siglo XX durante la guerra de guerrillas en Filipinas. Combinaron la "atracción" y "castigo" contra los insurgentes con una acción cívica deliberada como la construcción de infraestructuras, la educación, el mejoramiento de las capacidades de las fuerzas de seguridad. (Grubbs y Forsyth, 2005, p.29).

En la actualidad el grupo terrorista Sendero Luminoso puede considerarse como extinto. El último reducto liderado por los hermanos Quispe Palomino no puede considerarse senderista sino más bien una banda armada que sirve al narcotráfico. Así, para obtener financiación los hermanos Quispe Palomino brindan seguridad a los que transportan la cocaína por la selva cobrándoles entre tres y cinco dólares por kilo. También protegen las llamadas "narcopistas" en las que las avionetas pueden cargar hasta 300 kilos de cocaína por vuelo. Los analistas creen que si los hermanos Quispe Palomino atentan contra bases policiales y militares lo hacen para parecer fuertes y necesarios para los narcotraficantes.

Dejando a un lado los errores y los aciertos del gobierno peruano y las fuerzas de seguridad del Estado lo cierto es que este conflicto dejó unos 69.000 muertos y desaparecidos, según un informe de la Comisión de la Verdad y Reconciliación del año 2003. Una triste estadística que nos enseña hasta qué punto es importante conocer, entender y saber actuar frente a las tácticas terroristas y tratar de reducir así el sufrimiento de la población civil.

4. CONCLUSIONES

Siempre me ha parecido interesante que el teórico militar prusiano Carl von Clausewitz definiera la guerra en su obra cumbre, a principios del siglo XIX (cuando apenas existían los conflictos asimétricos a los que hoy asistimos), como "un verdadero camaleón". Todo parece indicar que el genial filósofo y teórico militar estaba adelantando lo que pasaría dos siglos después.

El terrorismo se inscribe dentro de la amalgama de los conflictos asimétricos y, como bien apuntaba el teórico militar prusiano, es polimorfo. Para un grupo terrorista saber adaptarse y aprender rápido es fundamental para su misma supervivencia. A su vez, las fuerzas y cuerpos de seguridad del Estado y los servicios de inteligencia también deben saber adaptarse para superar las dificultades impuestas y lograr combatir al enemigo y más cuando los malos solo tienen que tener suerte una vez y los buenos la tienen que tener siempre.

Como hemos comprobado, los terroristas, independientemente de su ideología política o religiosa y de los objetivos buscados, han sabido adaptar a sus propósitos una antigua táctica militar basada en el factor espacio, aunque la aplicación concreta en cada caso reviste particularidades que dependen tanto de las características del grupo terrorista como de las circunstancias.

Hemos ejemplificado su uso en dos casos históricos protagonizados por dos grupos terroristas diferentes que han empleado la táctica de negación de área, implementándola mediante medios y mecanismos distintos. El caso de ETA en España nos sitúa de bruces con la realidad angulosa de la diplomacia y las relaciones internacionales. Suele decirse, con razón, que en las relaciones internacionales no hay aliados sino intereses comunes que coinciden durante un tiempo y este caso parece ponerlo de manifiesto.

El caso de Sendero Luminoso en Perú nos sitúa ante un grupo terrorista que supo sacar partido de lo único que tenía a su favor, esto es, el factor geográfico y el conocimiento del medio y, al menos en los primeros años del conflicto, hizo de la selva peruana un lugar infranqueable para las tropas gubernamentales. A pesar de los errores descritos en cuanto a utilizar una estrategia militar sin acompañarla de otros medios económicos y de desarrollo en las zonas rurales, las fuerzas de seguridad supieron implementar y sacar provecho de la kingpin strategy, logrando ralentizar la operatividad del grupo terrorista y sembrando el desconcierto y las luchas internas por el poder.

Lo paradójico de la guerra de guerrillas es que ese término tuvo su origen en España durante la invasión de Napoleón Bonaparte en el siglo XIX, cuando fueron los propios ciudadanos los que se alzaron en armas contra el ejército regular francés para conquistar la libertad. Esto nos enseña cómo las mismas tácticas pueden usarse indistintamente para liberar al pueblo o para atenazarlo mediante el miedo y el terror.

BIBLIOGRAFÍA

ANTEZANA, J.(2012). *La caída de Artemio*. Instituto de Estudios Internacionales, Perú. Boletín nº 47. Disponible en la web: http://idei.pucp.edu.pe/la-caida-de-artemio/

GRUBBS, L.K y FORSYTH, M.J. (U.S. Army) (2005). *Is there a deep fight in a counter-insurgency?*. Military Review, Julio-Agosto de 2005. Disponible en la web: http://www.au.af.mil/au/awc/awcgate/milreview/grubbs.pdf

HERRERA, J.D.(2009). *Cooperación Franco-española frente al Terrorismo de ETA durante los gobiernos de José Luis Rodríguez Zapatero, Jacques Chirac y Nicolás Sarkozy*. Universidad del Rosario, Bogotá (Colombia).

JORDAN, J. (2009). *When heads roll: Assessing the effectiveness of leadership decapitation*. Security Studies, vol.18(4), pp. 719-755

SANCHEZ, M.A. (2016).*Cómo la Guardia Civil derrotó a ETA.* Cuadernos de la Guardia Civil (76 Aniversario del Servicio de Información), pp. 31-46. Disponible en la web: http://intranet.bibliotecasgc.bage.es/intranet-tmpl/prog/local_repository/documents/18268.pdf

SOMIEDO, J.P. (2015). *La estructura y la organización de los grupos terroristas bajo la óptica del aprendizaje organizacional*. Instituto Español de Estudios Estratégicos. Disponible en la web: http://www.emad.mde.es/DOCUMENTOSINTERES/documentos/

documentosEMAD/listado/151007-ESTRUCTURA-Y-ORGANIZACION-GRUPOS-TERRORISTAS.html

VV.AA. *Informe final de la Comisión Verdad y Reconciliación*. Disponible en la web: http://www.derechos.org/nizkor/peru/libros/cv/ii/ori.html

Elementos multimedia consultados:

Documental sobre la historia de ETA "Los años de Plomo": https://www.youtube.com/watch?v=w8yrodu0DX0

ETA y la Iglesia vasca: https://www.youtube.com/watch?v=yjvOWEOV3Q0

La captura de Feliciano: https://www.youtube.com/watch?v=GfK-TGDQh7g

Conversando con Sendero luminoso en la VRAE: https://www.youtube.com/watch?v=NKsx76ufmBw

Fecha de recepción: 11/11/2016. Fecha de aceptación: 20/12/2016

PATRIA

FERNANDO ARAMBURU

Editorial: TUSQUETS EDITORES, 2016, 648 páginas.

ISBN: 9788490663196

"Patria", de Fernando Aramburu, es una novela que debía ser escrita. Relatar los efectos producidos por la banda terrorista ETA en la sociedad del País Vasco, las complicidades, los silencios, los miedos y las cobardías, suponía un magnífico material para el relato. Pero no todo contenido era válido, tampoco servía cualquier forma de narrarlo y explicarlo. Y la sensibilidad hacia el asunto podía hacer que los efectos resultaran contraproducentes. Fernando Aramburu lo ha logrado, con una fórmula que,pese a su sencillez, parece irrepetible.

Aramburu, nacido en San Sebastián en 1959, y residente en Alemania desde 1985, ya había tratado tangencialmente el tema del terrorismo en obras previas, como "Fuego con limón" (1996), el libro de relatos "Peces de la amargura" (2006) o "Años Lentos" (2012). Ganador de diversos premios literarios, como el Euskadi, el Mario Vargas Llosa, el de la Real Academia Española, el Tusquets o el de Biblioteca Breve.

El libro de Aramburu permite una lectura a varios niveles. Desde una visión más superficial nos describe la vida, durante varias décadas, de dos familias destrozadas por el terrorismo, la del asesino y la de la víctima. Desde este punto de vista la obra resulta magistral, una novela de personajes, dibujando el autor a nueve protagonistas perfectamente caracterizados. Por un lado, la familia de José Mari, miembro de ETA, dirigida por Miren, la *ama* dura e intransigente, por el sumiso y cobarde *aita* Joxian, y por sus hermanos Arantxa, crítica con la acción armada, y Gorka, un aspirante a escritor. Por otra parte la familia del Txato, el empresario asesinado por ETA, comandada también por la *ama* Bittori y sus hijos Xabier, prisionero de la historia, y Nerea, que se niega a que su vida quede condicionada por ETA, especialmente tras haber coqueteado con el entorno abertzale en su juventud. Riqueza de matices en los personajes, pensamientos y acciones de los mismos que Aramburu suelta como latigazos, en frases cortas, directas, como golpes al cerebro en ocasiones y ganchos al hígado en otras.

A un nivel intermedio nos muestra el amplio catálogo de temáticas relacionadas con el terrorismo de ETA, algo que algunos han tratado de sustantivar como el "conflicto" vasco. Es terrorismo, sin más. Ejercicio de violencia, orientado a la generación de terror e intimidación, con objeto de cambiar el orden establecido. Personas cotidianas que por ser guardias civiles o policías eran tiroteadas; políticos o empresarios vascos, amantes de su "patria", extorsionados, agredidos, secuestrados o ejecutados; niños y jóvenes que estaban en el lugar y momento inadecuado; chavales atropellados por el poder de la masa, su cuadrilla, para nutrir la *kale borroka.* Asesinos y víctimas, pero no conflicto. Víctimas inocentes todas ellas, al margen de su origen, lengua, edad o profesión. Víctimas de la barbarie y la sinrazón.

Aramburu no rehúye el tratamiento de aspectos que pudieran despertar las mayores sensibilidades: el denunciable papel de la Iglesia, la cobardía de una sociedad

atemorizada, la dispersión de presos, la tortura de detenidos, los GAL o el plan de reconciliación entre terroristas y víctimas. Para ello introduce en la historia pasajes históricos, como el asesinato de Gregorio Ordoñez o el atentado de Hipercor, o nombres de miembros y cabecillas de ETA.

Al nivel más profundo, "Patria" está centrada en el odio. Es un relato sobre el odio. Sus causas, sus facilitadores y potenciadores. La forma en que se alimenta, engullendo los corazones y las almas de personas aparentemente buenas y racionales. La forma en que se construye sobre una narrativa, basada en "aquí y allí", el País Vasco y el Estado español, en "ellos y nosotros", en "buenos y malos", en agravios, objetivos o subjetivos. Los efectos del odio, desde la confrontación directa a la insensibilidad más absoluta, pasando por la invasión de todas las dimensiones de la cotidianeidad de los afectados. Y los resortes que hacen tremendamente compleja la salida del mismo.

El odio no viaja solo. Siempre viene acompañado. "Patria" es también una novela sobre la soledad, un clásico efecto del odio. Soledad de los personajes, a pesar de estar centrada en dos familias forjadas en un fuerte matriarcado. Hombres y mujeres que se niegan a ser felices, como Xabier, el hijo del Txato. Vidas rotas que se manifiestan de formas diferentes. Racionalidad versus irracionalidad. La psique humana construyendo realidades alternativas. Empatía, entendida como el esfuerzo por ponerse en el lugar del otro, tratando de entender sus motivaciones, deseos o expectativas. Empatizar, no simpatizar.

Y el perdón. El perdón como forma para enterrar el odio. El perdón como sanación del daño causado/sufrido. Por supuesto, una opción, tremendamente personal y voluntaria. El perdón como redención, liberación y reinicio.La dificultad para pedir perdón y para perdonar. Actos de valentía.

A nivel literario "Patria" es una maravilla. 125 capítulos breves, más de 600 páginas, en las que cuesta encontrar elementos que sobren o que falten. Ausencia de linealidad, con saltos temporales, entrecruzando las historias paralelas de las dos familias. Frases directas y cortas, en un estilo que recuerda a Azorín, lenguaje sencillo, ningún abuso descriptivo. Aramburu juega con recursos estilísticos, como la utilización de sinónimos separados por una barra, para potenciar los pensamientos de los protagonistas, frases que parecen sin acabar, como los pensamientos que afloran en la mente y se desvanecen al ser sustituidos velozmente por otros, diálogos sin atribución previa a personajes que el propio lector asigna posteriormente si el autor no lo hace.

Aramburu, como ya ha sido señalado en otras reseñas, ha escrito la gran novela española del siglo XXI. Un clásico que no cabe etiquetar en el posible género de novelas sobre terrorismo, que ya va presentando un amplio catálogo. Un libro que debería ser leído por alumnos de instituto y recomendado por sus profesores de literatura, al igual que en su momento leíamos "Nada", de Carmen Laforet, "El árbol de la ciencia", de Pío Baroja, "Las uvas de la ira", de Steinbeck, o "Guerra y Paz", de Tolstoi. Y, con mayor motivo, una novela de obligada lectura para profesionales de la seguridad o para candidatos a oficiales de la Guardia Civil.

Aramburu ha contado una parte importante de la historia de España y del País Vasco. Una labor a completar, para que jóvenes y futuras generaciones sepan qué pasó. El terrorismo de ETA no ha llevado a nada. La banda criminal está acabada y no ha conseguido ninguno de sus objetivos. Han sido derrotados/vencidos. Y se ha realizado

a través de la unidad de todos y con las herramientas del Estado de Derecho. En algún momento no fue así, pero es el respeto a la legalidad y los derechos humanos una de las características que nos hacen diferentes, que permite distinguir entre buenos y malos. Aunque el coste de la irracionalidad ha sido muy elevado. Ha costado, tomando las palabras de Churchill, sangre, sudor y lágrimas. Sangre de nuestros caídos, del dolor de familias ante la pérdida de padres, hermanos, hijos. Sudor por el esfuerzo desarrollado en la lucha contra ETA. Y lágrimas, muchas lágrimas… nunca deberíamos perder la capacidad de llorar ante las atrocidades que se comenten en este mundo. La Guardia Civil sabe bien de eso. Solo el tiempo podrá sanar las heridas, aunque, como se señala en la obra, las cicatrices no se puedan eliminar. Pero mientras que las heridas nos limitan, las cicatrices permiten vivir el día a día con elevado grado de normalidad. Aunque nunca se deba olvidar. Convivencia, en paz, en ese País Vasco que tan profundamente ama/siente Fernando Aramburu.

José María Blanco Navarro
Director del Centro de Análisis y Prospectiva
Guardia Civil

BITCOIN: LA TECNOLOGÍA BLOCKCHAIN Y SU INVESTIGACIÓN

FÉLIX BREZO Y YAIZA RUBIO

Editorial: 0xWorld, 240 páginas.

ISBN: 9788461769797

Yaiza Rubio y Félix Brezo son expertos en seguridad informática, "hackers" como a ellos les gusta llamarse, alejándose de las connotaciones negativas que habitualmente se vinculan al término, además de analistas de inteligencia y seguridad. Desarrollan su actividad profesional en Eleven Paths, la división de ciberseguridad de Telefónica desarrollada por el popular Chema Alonso.

En 2012, en unas jornadas organizadas por el Instituto Universitario de Investigación en Seguridad Interior (IUISI), de la UNED y la Guardia Civil, fui encargado de desarrollar una ponencia sobre tendencias en materia de blanqueo. El asesoramiento previo del Dr. Félix Brezo me permitió realizar una aproximación sobre Bitcoin. En agosto de ese mismo año el IUISI había publicado un artículo suyo titulado "Aplicaciones ciberdelictivas de criptodivisas como Bitcoin", que resultó pionero en el tratamiento de estos temas en España. En 2013 se decidió que era la persona adecuada para profundizar en estas cuestiones en el II Seminario sobre el Delito de Blanqueo, organizado de nuevo por el IUISI.

Yaiza y Félix colaboran habitualmente con el Centro de Análisis y Prospectiva de la Guardia Civil, formando parte de su grupo de trabajo en materia de prospectiva. Han ofrecido formación especializada a miembros de diferentes organizaciones de seguridad, incluyendo a unidades especializadas de la Guardia Civil. También participan en programas de postgrado de diferentes universidades, especialmente en el Instituto de Ciencias Forenses y de la Seguridad (ICFS) de la Universidad Autónoma de Madrid. Colaboran habitualmente en jornadas y seminarios, como el Curso de Verano de la Guardia Civil de 2016, tratando el uso de nuevas tecnologías para contrarrestar su uso por organizaciones criminales. En esa línea han desarrollado la aplicación de código abierto OSRFramework[1].

Quienes conocemos a Yaiza y Félix sabemos de su absoluto compromiso con la seguridad de nuestro país, su continua disponibilidad para apoyar la acción de las organizaciones públicas y sus enormes capacidades para conjugar conocimiento muy especializado, desarrollo de utilidades y capacidades didácticas para hacernos comprender tanto los riesgos como las oportunidades que se derivan del uso de nuevas tecnologías.

El volumen que nos ofrecen explica tanto el funcionamiento de las criptodivisas, entre las cuales Bitcoin es la más conocida, como la tecnología Blockchain, que da soporte al sistema. Desde que un artículo titulado "Bitcoin: A Peer-to-Peer Electronic Cash System" explicase los fundamentos de Bitcoin como protocolo público y al año siguiente se lanzase la moneda, generándose los primeros bitcoins y realizándose las primeras transacciones, han sido infinidad las criptodivisas que han ido surgiendo, tal

1 https://i3visio.com/

y como van mostrando los autores de este libro. Y estos nuevos sistemas de pago alternativos también han sido adoptados por los criminales, por su “anonimato”. Pero obviando este detalle, poseen multitud de utilidades, que Yaiza y Félix nos van desgranando a lo largo de sus páginas. De hecho entidades bancarias tradicionales, como BBVA y Bankinter, entre otras, están invirtiendo en esta tecnología desde diferentes perspectivas del negocio, tal y como nos señalan los autores. Y es que son un medio de pago seguro y hacer transacciones con ellas no conlleva prácticamente ningún coste adicional. Además se puede alternar su uso con el dinero convencional, también se usan como unidad de cuenta y es un medio que sirve para almacenar valor. De hecho, nos cuentan que Bitcoin por ejemplo, posee un límite máximo de 21 millones de bitcoins puestos en circulación, por lo que no tenderá a la inflación como otros activos.

Blockchain, o la cadena de bloques, se puede definir como un registro distribuido, con ficheros compartidos por miles de ordenadores, que hace imposible su alteración de forma malintencionada. En ese sentido se configura como un nuevo modelo de negocio. Incluso la directora del Fondo Monetario Internacional, Christine Lagarde, cree que las instituciones financieras deberían adoptar este tipo de tecnologías digitales, que pueden prevenir los delitos financieros y el blanqueo de capitales. Modelos de gestión que podrían ser aplicados igualmente a las telecomunicaciones o al sector público, o a la suscripción de smart contracts, y no precisarían la supervisión de un verificador. Toda una serie de ventajas que los autores de este libro nos ayudan a conocer, adentrándonos en los detalles más desconocidos para el común de los mortales.

Bitcoin, criptodivisas, minería o cadena de bloques son conceptos que se van cruzado en nuestro camino, tanto en medios de comunicación como webs especializados. Las oscilaciones en su cotización, su naturaleza descentralizada ajena al control de los estados y las posibilidades que ofrece para la realización de transacciones en la red hace tiempo que empezaron a atraer, por un lado a inversores grandes y pequeños y, por otro, a especialistas en seguridad y curiosos de la tecnología.

En la citada obra los autores tratan de responder a un cúmulo de preguntas que asaltan a quien es profano en la materia: ¿Cuánto vale un bitcoin?, ¿dónde puedo conseguirlos?, ¿hasta qué punto es anónimo el pago con bitcoins?, ¿y si los pierdo?, ¿puedo crearme mi propia criptodivisa?, ¿qué cosas puedo adquirir o comprar?, ¿qué puedo saber de una dirección y hasta dónde puedo rastrearla?, ¿de verdad la tecnología de Blockchain solucionará todos mis problemas?

A estas preguntas Yaiza y Félix ofrecen respuestas, con una visión tremendamente práctica, un estilo didáctico y el apoyo de tecnologías libres que tanto conocen, y que han posibilitado el desarrollo de una comunidad que va mucho más allá del sistema de pago descentralizado que empezó a incubar un aún desconocido Satoshi Nakamoto. Mientras tanto, la cadena de bloques sigue creciendo y sigue añadiendo operaciones cada diez minutos...

Al margen de sus conocimientos técnicos, la aportación fundamental de los autores es su proximidad al sentir del analista de seguridad, tratando de cubrir la enorme brecha existente en este mundo de la seguridad entre los tecnólogos y los usuarios finales. Ambos conocen perfectamente las necesidades de las organizaciones públicas y privadas. Son conscientes de las oportunidades existentes, además de los riesgos de las tecnologías. Y ofrecen soluciones para gestionar con inteligencia este mundo veloz, volátil y complejo, especialmente en el ciberespacio. Ese es el primer

paso para la búsqueda de tecnologías útiles y que no siempre exigirán un desembolso económico desorbitado.

José María Blanco Navarro
Director del Centro de Análisis y Prospectiva
Guardia Civil

FUTURE CRIMES
A JOURNEY TO THE DARK SIDE OF TECHNOLOGY - AND HOW TO SURVIVE IT

MARC GOODMAN

Great Britain: Bantam Press, 2015, 464 páginas.

ISBN: 9780593073650

Think about it, son las palabras que mejor resumen el objetivo que parece extraerse de la última obra de Marc Goodman quien invita, de manera cercana y directa, a reconsiderar nuestros hábitos diarios. Quien se cuestiona, desde el punto de vista de la oportunidad criminal, si la penetración que estamos permitiendo a la tecnología en nuestras vidas se puede volver en nuestra contra.

Goodman, formado en administración pública en la Universidad de Harvard y en gestión de sistemas de la información por la London School of Economics, es un reconocido consultor en materia de seguridad que ha trabajado, entre otros, como asesor principal del Comité Directivo de Interpol en Crimen de la Tecnología de la Información. Cargo que le ha permitido formar parte de la capacitación impartida a policías de medio mundo. Miembro del Centro Internacional de Seguridad y Cooperación de la Universidad de Stratford, uno de los principales reconocimientos a su labor ha sido su nombramiento como parte del grupo de expertos en la Unión Internacional de Telecomunicaciones de Naciones Unidas.

Su labor divulgativa abarca más de una docena de artículos en prestigiosas revistas y publicaciones, cuyo elemento común subyace claramente; las amenazas emergentes. Tal es su interés por el tema que ha fundado el Instituto de Crímenes del Futuro como foro de discusión sobre la seguridad, el crimen y la tecnología, el cual ya dispone de más de 1.000 miembros en 37 países.

Esta obra forma parte del creciente y atractivo repertorio bibliográfico que expone consecuencias, eminentemente sociales, de las nuevas tecnologías. Una temática abordada con anterioridad en sugestivas publicaciones como: *Is Google making us stupid?* de Nicholas Carr (2008), *Alone Together* escrita por Sherry Turkle (2011), *Públicamente avergonzados*, redactada por Jon Ronson (2015) o *El futuro digital*, de Eric Smith y Jared Cohen (2015). Estas, y muchas otras obras, están conformando una suerte de género de ficción, con una base de realidad documental al que no le falta un buen aliño distópico. Definiciones nada nuevas si traemos a colación la cita de uno de los más grandes futuristas, el recientemente fallecido Alvin Toffler quien, no ajeno a discusiones de esta envergadura, auguraba en *La Tercera Ola* (1979) que "*una de las definiciones de cordura es la capacidad de distinguir lo real de lo irreal. Pronto necesitaremos una nueva definición"*.

Future Crimes se presenta cual diagnóstico sobre los peligros que encierra el uso de las nuevas tecnologías cuando se emplean en modos y formas no adecuados, irguiéndose así en tecnologías de doble uso en términos criminológicos. En este sentido, cada evolución, en lo que a tecnología respecta, puede estar asociada a negativos

escenarios cuya mínima consideración obviamos. De este modo, nuestro día a día en la red actúa a modo de fertilizante de la criminalidad.

No apto para quienes sucumben con facilidad a la ansiedad. Y no es que caiga en la negatividad sistemática, sino que genera un debate reflexivo donde las desventajas de las nuevas tecnologías, particularmente enfocadas en el futuro de la delincuencia y el terrorismo, cobran protagonismo en detrimento de las ventajas. Donde expone este tipo de incidentes como la nueva normalidad, tratando de concienciar que se dejen de considerar aislados.

Ataques terroristas facilitados por el uso de redes sociales, las mismas que son empleadas para vulnerar la privacidad de sus usuarios; robos masivos en registros bancarios; uso de malware encubierto en terceros servicios; hacking de los dispositivos médicos implantados en el cuerpo humano; venta de historiales médicos; penetración en los teléfonos personales; ataques a grandes sistemas eléctricos. Una fluida integración entre escenarios conocidos y plausibles, con una fantasía futurista muy real.

Lo llamativo es el elenco de detallados ejemplos expuestos, ya pasados, actuales o hipotéticos, que invitan al lector a pensar que pasará cuando algunos de estos escenarios se extiendan a nuestra casa, vehículo, empresa o cuerpo. Es quizás en esta parte, la de las respuestas, donde la lectura pierde fuerza, pues se deja a la imaginación del lector toda implicación. Al igual que sucede con las recomendaciones dadas, que descansan en la ya hiper aludida necesidad de uso de contraseñas más largas y acceso solo a lugares seguros, a todas luces, recomendaciones poco sofisticadas a tenor de los escenarios en que nos sumerge. Más interesante resulta su apuesta por la creación de un organismo internacional bajo el cual se coordine y comparta información sobre todos los ataques cyber que se den que, si bien no es una medida nueva, podría tener positivos resultados en lo que a prevención respecta, pese a lo utópico de su existencia. Insta igualmente al sector público y privado a trabajar más estrechamente, pero también a hacer partícipe a la población, alegando que la seguridad pública es demasiado importante como para dejarla (solo) en manos de los profesionales. Reivindica la alfabetización digital de la sociedad como pilar fundamental de un futuro menos vulnerable.

Un efecto inmediato es la activación de esa relegada zona de nuestro cerebro que nos permite pensar en situaciones no conocidas. Y es que la tecnología es nueva, pero el crimen no, y no resulta nada descabellado pensar en las implicaciones que este último puede tener cuando se sirve de una herramienta a la que le hemos abierto todos nuestros límites conocidos. Quizás, por esa falsa seguridad bajo la cual no nos creemos atractivos como posibles objetivos para acciones delictivas. El error está en no advertir que estas son cada vez menos personales, más masivas, más indiscriminadas y, potencialmente, más dañinas.

Es destacable igualmente su visión sobre la criminalidad futura como entidad institucionalizada. Organizaciones que operan a modo de grandes empresas del crimen capaces de realizar acciones de envergadura superior a la de cualquier estado o multinacional que actúen en la legalidad. Alude este escenario como el inicio de la “gran época de la delincuencia digital”. Nada lejos de la criminalidad organizada de la que ya somos testigos en nuestros días, aunque potenciada en cuanto capacidad y efectos.

El inconsciente, a cada página leída, graba su propio mensaje: a mayor dependen-

cia, mayor exposición al riesgo, de ahí su llamada a iniciar, desde el mismo momento en que se cierran sus lomos, una adecuada prevención. Una respuesta asentada en la capacidad de ver nuestra realidad desde la perspectiva del juicio crítico, de interiorizar que nuestra realidad no es un bien privado, de entender que la realidad ya no es lo que era, es efímera y puede ser muy dañina.

Jessica Cohen
Analista en Seguridad Internacional

DATOS SOBRE LOS AUTORES DE ESTE VOLUMEN POR ORDEN ALFABÉTICO

José Ángel Astillero Fuentes es Teniente Coronel Diplomado de Estado Mayor. Ha desarrollado la mayor parte de su carrera en los ámbitos de la cooperación policial internacional, el antiterrorismo y la docencia. Está en posesión del Máster en Dirección General y Planificación Estratégica (ESERP Business School, 2011), del Máster de Seguridad (2010) y del Máster en "Cooperazione e Sicurezza Internazionali"(Libera Università Maria S.S. Assunta, 2002). Además tiene estudios de postgrado en el campo de la seguridad, las relaciones internacionales y el management. Desde 2013 está destinado en el Servicio de Costas y Fronteras de la Dirección General de la Guardia Civil. jaastillero@guardiacivil.es

María José Garrido Antón, Capitán de la Guardia Civil, destinada en la Sección de Análisis del Comportamiento delictivo (SACD) de la Unidad Técnica de Policía Judicial (UTPJ). Doctora en Psicología por la Universidad Autónoma de Madrid con mención Europea por la "Mitt Swedish University", con una Tesis que lleva por título " Validación del procedimiento de valoración del riesgo de los casos de violencia de género del Ministerio del Interior de España" (2012). Master en Ciencias Forenses por la Universidad Autónoma de Madrid y experta en Criminología. A nivel académico es autora de varios capítulos de libro y de algunos artículos científicos, ha participado en diversos proyectos de investigación y en decenas de ponencias y comunicaciones a congresos. Es miembro del Instituto de Ciencias Forenses y de la Seguridad (ICFS) de la Universidad Autónoma de Madrid, donde colabora como docente en algunas de sus actividades formativas. mjganton@guardiacivil.es

José Luis González Álvarez, Comandante de la Guardia Civil, con funciones de Policía Judicial Específica desde finales de los 80. Doctor en Psicología con una tesis sobre la aplicación policial de la Entrevista Cognitiva en España (2005). Master en Ciencias Forenses (UAM). Fundador en 1995 de los Equipos Mujer Menor (EMUMEs) y de la Sección de Análisis del Comportamiento Delictivo (SACD) de Policía Judicial GC, ha trabajado en los últimos 25 años en la aplicación sobre el terreno de los conocimientos de la psicología a las tareas de investigación criminal, en el desarrollo de la rama de la Psicología Criminalista dentro de la Psicología Jurídica, impulsando el análisis profesional de la conducta en beneficio de las investigaciones criminales. Autor de varios libros y artículos científicos, ha participado en diversos proyectos de investigación científica y de cooperación policial nacionales e internacionales, y su interés profesional y científico se centra en el desarrollo de protocolos prácticos para facilitar a los agentes policiales su labor (desarrollando el Sistema VioGen del Ministerio del Interior). Impulsor de la creación del Instituto de Ciencias Forenses y de la Seguridad de la Universidad Autónoma de Madrid, colabora desde su origen como docente; también con otras Universidades y Centros de Investigación científica y en las actividades formativas internas de la Guardia Civil y de otras FCS en Policía Judicial. Está destinado en la Secretaría de Estado de Seguridad. jlga@interior.es; joseluisalvarez@guardiacivil.es.

Rafael Hernández Alonso está destinado en el Servicio de Estudios Históricos de la Guardia Civil desde 2009. Es licenciado en Historia por la Universidad Nacional de

Educación a Distancia (UNED) y Especialista Universitario en Historia Militar, por el Instituto Universitario Gutiérrez Mellado-UNED. Asimismo está en posesión de diferentes cursos, relacionados con la Historia Militar de España, Uniformología, historia del Armamento, sobre heráldica militar o vexilología militar española, entre otros. rhalonso@guardiacivil.es

Rodrigo Lodeiro Corral es Comandante de la Guardia Civil. Está destinado en el Estado Mayor de la Guardia Civil y es el Oficial de Enlace con el Mando de Operaciones del Estado Mayor de la Defensa, donde ejerce como analista de las operaciones militares en el exterior. Ha estado a cargo de la Sección de Investigación Criminal de la Unidad Orgánica de Policía Judicial de la Comandancia de La Coruña y de la Sección de Información de la Zona de la Guardia Civil de Galicia. Posee los Másteres Universitarios en Política de Defensa y Seguridad Internacional por la Universidad Complutense de Madrid, de Seguridad por la Universidad Nacional de Educación a Distancia y en Prevención de Riesgos Laborales por la Universidad Camilo José Cela. Colabora como docente con la Academia Galega de Seguridad Pública, donde se realiza la formación de los diferentes Cuerpos de Policía Local de Galicia. rlodeiro@guardiacivil.es

Eva Martín Ibáñez, Doctora por la UCM (Ciencias de la Información), Master en Análisis de Evidencias Digitales y Lucha contra el Cibercrimen (UAM), MBA por el Instituto de Empresa (IE Business School), licenciada en Derecho (UCM), licenciada en Ciencias Políticas y Sociología (UNED), y título de experto en Análisis de Inteligencia (UAM). Actualmente trabaja como periodista especializada en tecnología y economía. Ha sido consultor en proyectos de radiodifusión, telefonía móvil, televisión digital y transporte. Ha co-escrito una docena de libros, dos de ellos sobre seguridad informática básica. 88wz88@gmail.com

Juan Pablo Somiedo es analista estadístico y profesor de metodología de análisis en Inteligencia en el Curso de Experto en Inteligencia de la Universidad Autónoma de Madrid. Ha sido capellán militar con la consideración de capitán ocupando destinos en la Unidad Militar de Emergencias (UME), el Estado Mayor de la Defensa (EMAD) y el Centro Superior de Estudios de la Defensa Nacional (CESEDEN) donde se especializó en inteligencia estratégica. Es licenciado en Estudios Eclesiásticos por la Universidad Pontificia de Salamanca, Grado en Estadística por la Universidad Carlos III de Madrid, Master Oficial en Lógica y Filosofía de la Ciencia por la UNED y Magister en Seguridad y Defensa con especialización en inteligencia por el CESEDEN. Además ha cursado diferentes cursos de especialización en el ámbito de la inteligencia. jupasom@yahoo.es

NORMAS PARA LOS AUTORES

Los trabajos que se remitan para su publicación en la Revista "Cuadernos de la Guardia Civil" deberán ser inéditos y no estar pendientes de publicación en otra revista. No obstante, previa solicitud al Centro de Análisis y Prospectiva, podrán ser publicados en otro medio, una vez otorgada autorización escrita en tal sentido por el Director de la revista.

Los criterios para la presentación de textos son los siguientes:

EXTENSIÓN. Un mínimo de 6.000 palabras y un máximo de 9.000 a espacio y medio, en DIN A-4.

TÍTULO, AUTORÍA Y AFILIACIÓN. En la primera página constará el título, en mayúsculas y negrita, y, debajo, el nombre del autor (en mayúsculas), indicando puesto de trabajo y profesión.

Se adjuntará adicionalmente breve CV del autor de 10 o 15 líneas y dirección de correo electrónico.

RESUMEN Y PALABRAS CLAVE. Precedido de la palabra "Resumen" se incluirá a continuación un extracto en castellano de unas 10-15 líneas. A continuación, en otro párrafo, un "Abstract", traducción al inglés del resumen anterior. En el párrafo siguiente se incluirán las palabras clave, en un máximo de cinco, precedidas por la expresión "Palabras clave". A continuación, en párrafo nuevo, esas palabras clave en inglés precedidas de la expresión "Keywords".

ESTRUCTURA. Los trabajos se dividirán en apartados y secciones (2 niveles), con su propio título, numerados. Se titularán en mayúscula negrita en el primer nivel de jerarquía y con mayúscula redondo en el segundo (sin negrita). Si fuera necesario un tercer nivel se escribiría en minúscula y negrita, y el cuarto en minúscula y cursiva.

TIPO DE LETRA. Arial 12 puntos. Las notas y afiliación serán de la misma letra, tamaño 10 puntos.

CUADROS Y FIGURAS. Serán numerados e incluirán una breve titulación.

PÁRRAFOS. Sangrado de 5 espacios. Espacio sencillo.

Se evitará la utilización de negrita y palabras subrayadas en el cuerpo del texto. Se utilizará letra cursiva para los títulos de libros y otras fuentes o para la inclusión dentro del texto de palabras o expresiones en otro idioma diferente al del artículo.

NOTAS. Serán las imprescindibles y se situarán al final de la página de forma numerada.

REFERENCIAS Y CITA BIBLIOGRÁFICA. Se utilizará el sistema APA (http://www.apastyle.org/ http://normasapa.com/)

- En el texto

Se utilizará el sistema APA, en el texto del artículo, para citar autoría y fecha, evitando en todo caso el uso de notas a pie de página. Ejemplo: (García, 2014) o "según García (2014) las condiciones…."

- Bibliografía

Se limitará a las fuentes bibliográficas utilizadas y referenciadas en el texto. Sigue orden alfabético de apellido de autores.

Ejemplos:

1. Libro:

Mansky, C. (2013). Public Policy in an Uncertain World. London: Harvard University Press.

2. Artículo o capítulo de libro:

Antaki, C. (1988). Explanations, communication and social cognition. En C. Antaki (Ed.), Analysing everyday explanation. A casebook of methods (pp. 1-14). London: Sage.

3. Artículo:

Moskalenko, S.; McCauley, C. (2010). Measuring Political Mobilisation: The Distinction Between Activism and Radicalisation. Terrorism and Political Violence, vol. 21, p. 240.

4. Artículo de revista on-line:

Blanco, J. M.; Cohen, J. (2014).The future of counter-terrorism in Europe. The need to be lost in the correct direction. European Journal of Future Research, vol. 2 (nº 1). Springer. Extraído el 1 de enero de 2015 de: http://link.springer.com/article/10.1007%2Fs40309-014-0050-9

5. Contenidos on-line:

Weathon, K. (2011). Let's Kill the Intelligence Cycle. Sources and Methods. Extraído el 1 de enero de 2015 de: http://sourcesandmethods.blogspot.com/2011/05/lets-killintelligence-cycle-original.html

6. Artículos o noticias de periódico:

Schwartz, J. (10 de septiembre de 1993). Obesity affects economic, social status. The Washington Post, pp. B1, B3, B5-B7

ORGANISMOS Y SIGLAS. Siempre que sea posible se utilizarán las siglas en castellano (OTAN, y no NATO; ONU y no UNO). La primera vez que se utilice una sigla en un texto se escribirá primero la traducción o equivalencia, si fuera posible, y a continuación, entre paréntesis, el nombre en el idioma original, y la sigla, separados por una coma, pudiendo posteriormente utilizar únicamente la sigla:

Ejemplo: Agencia Central de Inteligencia (Central Inteligencia Agency, CIA).

Se acompañará en soporte informático, preferentemente Microsoft Word. Las fotografías y ficheros se remitirán también en ficheros independientes. Se podrá remitir por correo electrónico a esta dirección: CAP-cuadernos@guardiacivil.org

Los trabajos se presentarán, precedidos por una ficha de colaboración en la que se hagan constar: título del trabajo, nombre del autor (o autores), dirección, NIF, número de teléfono y de fax, situación laboral y nombre de la institución o empresa a la que pertenece. Igualmente se presentará una ficha de cesión de derechos de autor, que se facilitará oportunamente.

Los artículos serán evaluados por el Consejo de Redacción. Se enviarán a los autores las orientaciones de corrección que se estimen pertinentes, salvo aquellas de carácter menor, que no afecten al contenido y que puedan ser realizadas por el equipo de redacción (correcciones de tipo ortográfico, de puntuación, formato, etc.).

Los autores de los trabajos publicados en la Revista serán remunerados en la cuantía que establezca el Consejo de Redacción, salvo aquellos casos en que se trate de colaboraciones desinteresadas que realicen los autores.

A todos los autores que envíen originales a la Revista "Cuadernos de la Guardia Civil" se les remitirá acuse de recibo. El Consejo de Redacción decidirá, en un plazo no superior a los seis meses, la aceptación o no de los trabajos recibidos. Esta decisión se comunicará al autor y, en caso afirmativo, se indicará el número de la Revista en el que se incluirá, así como fecha aproximada de publicación.

Los artículos que no se atengan a estas normas serán devueltos a sus autores, quienes podrán reenviarlos de nuevo, una vez hechas las oportunas modificaciones.

Los trabajos que se presenten deberán respetar de forma rigurosa los plazos que se indiquen como fecha máxima de entrega de los mismos.

Ni la Dirección General de la Guardia Civil ni "Cuadernos de la Guardia Civil" asume las opiniones manifestadas por los autores.

CENTRO UNIVERSITARIO GUARDIA CIVIL

Marco Legal

- Ley 39/2007 de la Carrera Militar
- Real Decreto 1959/2009 de creación del Centro Universitario de la Guardia Civil (CUGC)
- Orden PRE /422/2013 de servicios centrales de la DGGC
- Ley 29/2014 de Régimen de Personal de la Guardia Civil

Capacidades

- Titularidad del Ministerio del Interior a través de la Dirección General Guardia Civil.
- Ente público diferente de la Administración General del Estado.
- Adscrito a una o varias universidades públicas que expiden titulos oficiales universitarios del EEES: Actualmente UC3M y UNED.
- Impartir titulaciones universitarias oficiales (grado, máster, doctor) y desarrollar líneas de investigación de interés para la Guardia Civil.
- Acuerdos de cooperación con otras instituciones a nivel nacional e internacional.

Oferta Académica

Actualmente el CUGC está adscrito a la Universidad Carlos III de Madrid (UC3M) e imparte las Titulaciones Académicas oficiales de:

- Grado en Ingeniería de la Seguridad.
- Máster en Dirección Operativa de la Seguridad.
- Grado para la promoción interna de los Suboficiales de Guardia Civil (pendiente de acreditación).

Está pendiente de desarrollo, la adscripción del CUGC a la Universidad Nacional de Educación a Distancia (UNED).

Para prestar un mayor apoyo en las asignaturas y facilitar el contacto con los alumnos, el CUGC dispone de un Aula Virtual cuyo acceso se realiza desde la página web (www.cugc.es). Además desarrolla las siguientes actividades:

- Apoyo institucional para desarrollo de doctorados.
- Investigación Académica.
- Reconocimiento Carta Erasmus 2014-2020.
- Línea Editorial del CUGC.
- Extensión Universitaria.

Diciembre 2014 1º Promoción Ingenieros Seguridad

El **Instituto Universitario de Investigación sobre Seguridad Interior** se creó mediante la firma de un convenio de colaboración suscrito entre el Ministerio del Interior, la Dirección General de la Guardia Civil y la Universidad Nacional de Educación a Distancia, el 17 de octubre de 2002, pues la Guardia Civil y la UNED llevaban vinculadas por distintos acuerdos de colaboración desde 1988 y precisaban de un centro especializado en la investigación, enseñanza y asesoramiento en materias relacionadas con la seguridad.

IUISI pretende desarrollar y promover la investigación científica de alta calidad en materias de seguridad que sean de interés para instituciones públicas y privadas, impulsar y promover la difusión de obras científicas, y crear un marco de reflexión y diálogo.

Las actividades previstas para este año se irán anunciando en su página web: www.iuisi.es