SEC2CRIME

FROM SECURITY TO CRIME PREVENTION

MEMORIA 2021

#SomosSec2Crime

Índice

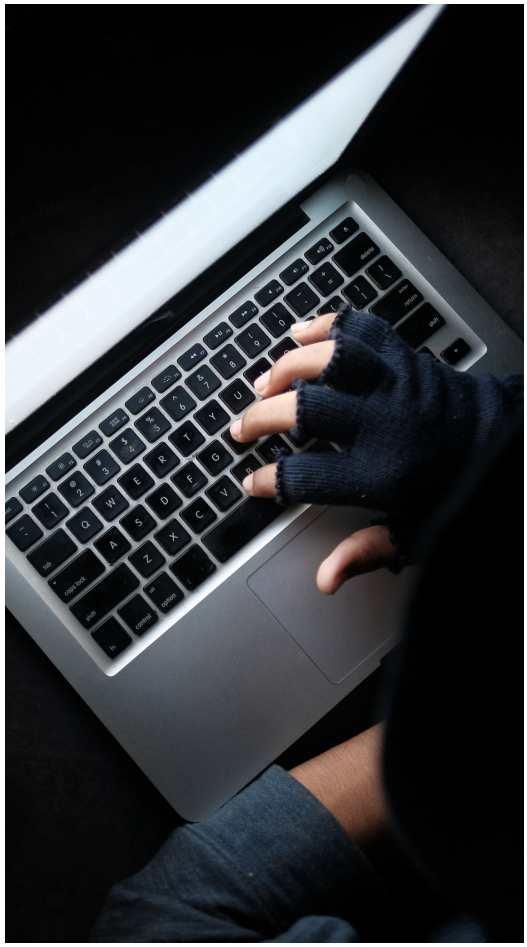
SEC2CRIME
FROM SECURITY TO CRIME PREVENTION

01
NOSOTROS
¿Quiénes somos?
Presentación de Sec2Crime.

04
ARTÍCULOS
Publicaciones destacadas de nuestros colaboradores.

77
EVENTOS
Eventos realizados por la entidad durante el año.

80
ENTREVISTAS
Hablamos con nuestro Comité de Expertos.



Nacimos para revolucionar el sector Seguridad

Sec2Crime® -From Security to Crime Prevention- es una entidad innovadora del sector Seguridad que nació en mayo del año 2020.

Lo que empezó como una idea enfocada en demostrar el valor de la criminología en la sociedad actual, se ha ido consolidando también como una entidad de referencia en otras áreas, como la Ciberseguridad, el Análisis de inteligencia, la Defensa nacional o los Conflictos Armados y la prevención del Terrorismo.

En este sentido, su equipo directivo apuesta, por un lado, por una dimensión divulgativa (think tank), basada en una comunidad profesional y en la investigación independiente; y, por otro, por un enfoque empresarial, aún en fase de explotación. Para lograr sus objetivos cuenta, además de con más de 50 colaboradores -divididos en distintas áreas temáticas-, con un importante apoyo institucional, tanto de escuelas y universidades, como empresas privadas, asociaciones y colegios profesionales (www.sec2crime.com/equipo).

A través de su página web (www.sec2crime.com) y sus redes sociales (@sec2crime) se puede intuir el grueso de su actividad, así como la diferenciación que ofrecen y el valor que pretenden aportar: un blog dividido en segmentos del conocimiento, en el que se puede encontrar tanto información general sobre determinadas temáticas, como salidas profesionales, formación, artículos profesionales (más de 250 en total) e incluso libros y bibliografía recomendados; proyectos de investigación y trabajos ya editados -muchas veces en colaboración con sus partners-; eventos y talleres periódicos; post y contenido audiovisual; servicios y productos del sector; y un amplio amalgama de contenido gratuito, dando a conocer, por ejemplo, revistas y entrevistas propias.

Otro de los puntos fuertes de esta entidad es su Método 2.0, un sistema de aprendizaje online basado en documentos de elaboración propia y entrevistas con profesionales de distintos sectores vinculados a la Seguridad repartido en módulos, con el que buscan "aportar conocimiento en línea, de forma gratuita y con valor diferencial para el desempeño profesional". Además, al finalizarlo "podrás recibir un certificado de aprovechamiento sobre contenido práctico y descuentos para especializarte con los mejores".

Por otro lado, Sec2Crime ha constituido, recientemente, un Comité de Expertos, formado por perfiles de reconocida experiencia: **Eugenia Hernández,** Directora de UNINT (Unidad de Análisis de Inteligencia de la Universidad Autónoma de Madrid) y diplomada en Altos Estudios de Defensa Nacional (CESEDEN); **Matteo Re**, Doctor en Historia Contemporánea, investigador y Profesor en el Máster "Análisis y prevención del terrorismo" de la Universidad Rey Juan Carlos; **Paz Velasco de la Fuente**, Criminóloga y jurista especializada en personalidad psicopática y delitos violentos. Escritora y creadora de "Criminal-mente"; **Edo Bakker**, CEO de Agile Control Solutions. Asesor y Experto Externo registrado en Prevención del Blanqueo de Capitales y Compliance; y **Federico Aznar Fernández** Montesinos, Doctor en Ciencia Política, escritor, militar, ensayista y profesor universitario.

En definitiva, los principios de Sec2Crime son la **transparencia**, la **imparcialidad**, el impulso de proyectos a gran escala de difusión, concienciación y prevención y el mantenimiento de altos estándares de **calidad**, dado que los materiales elaborados reciben revisiones múltiples por parte de los colaboradores que integran cada área. Así, y poniendo de relieve que su equipo se encuentra en un continuo crecimiento interno y social, que se trata de un equipo joven y dinámico y que su formato de trabajo se basa en la creatividad, estamos seguros de que el esfuerzo dedicado contribuirá al desarrollo del sector.

David García Marín
CEO y fundador.
Criminólogo y Analista de Inteligencia

David Vargas Aguilera
Dirección Adjunta.
Criminólogo. Miembro de las FAS.

Pino Penilla Marquínez
Dirección Adjunta.
Analista de Ciberinteligencia.

Jacobo S. Micó Faus
Dirección Adjunta. Criminólogo.
Analista de Terrorismo.

© de la edición:

Sec2Crime®

Diciembre de 2021

28028 (Madrid) (España)

https://www.sec2crime.com

© de los textos:

Reservados todos los derechos. Tanto la totalidad como las partes de esta publicación no pueden reproducirse o transmitirse de ninguna forma o por ningún medio, sea electrónico, mecánico, reprográfico, fotoquímico, óptico, de grabación o cualquier otra forma de almacenamiento de información o sistema de recuperación, sin el permiso previo y por escrito de Sec2Crime.

ARTÍCULOS

Nuestros colaboradores contribuyen diariamente al desarrollo de Sec2Crime en su dimensión divulgativa/*think tank*. En este apartado hemos decidido compartir con ustedes algunos de sus artículos, publicados durante el presente año -2021- y vinculados a disciplinas y fenómenos relacionados con la Criminología, la Delincuencia Económica, la Prevención del Terrorismo, los Conflictos Armados, el Análisis de Inteligencia, la Ciberseguridad y la Defensa nacional.

La Alianza Atlántica y el principio de Defensa Colectiva

Resumen: el principio de Defensa Colectiva, recogido en el artículo 5 del tratado fundacional de la Organización del Tratado Atlántico Norte (OTAN), representa la piedra angular de su fundación y el lazo de unión entre los Estados miembros de la Alianza.

Este principio establece que un ataque armado contra uno o varios países miembros de la OTAN, acecido en Europa o América del Norte, "se considerará como un ataque dirigido contra todas ellas". Así, la Defensa Colectiva se convierte en un derecho y un deber que los países de la Alianza se comprometen a garantizar.

Hasta el momento, el artículo 5 ha sido invocado una única vez, en el año 2001, tras los atentados terroristas del 11-S contra las Torres Gemelas de Nueva York y el Pentágono de Washington.

INTRODUCCIÓN

El 2 de octubre de 2001, el Secretario General de la Organización del Tratado Atlántico Norte (OTAN), Lord Robertson, se dirigía a la Comunidad Internacional para anunciar, por primera vez en la historia, la invocación del artículo V del Tratado de Washington:

Sobre la base de esta información, se ha determinado que el ataque contra Estados Unidos del 11 de septiembre fue dirigido desde el extranjero y, por lo tanto, se considerará una acción cubierta por el artículo 5 del Tratado de Washington".

El principio de Defensa Colectiva, recogido en el artículo V del tratado fundacional de la OTAN, representa la piedra angular de su fundación y el lazo de unión entre los Estados miembros de la Alianza.

EL ORIGEN DE LA OTAN

El Tratado de Washington fue firmado en 1949 por diez países (Bélgica, Canadá, Dinamarca, Estados Unidos, Francia, Islandia, Italia, Luxemburgo, Noruega, Países Bajos, Portugal y Reino Unido) de ambos lados del Océano Atlántico dando origen a la Organización del Tratado Atlántico Norte, una alianza basada en el compromiso de defenderse mutuamente en caso de agresión armada a cualquiera de sus Estados miembros.

Así, nació la primera alianza entre países de América del Norte y Europa Occidental, basada en el derecho inherente de legítima defensa, individual o colectiva, en caso de ataque armado, recogido en el artículo 51 de la Carta de Naciones Unidas.

En la actualidad la OTAN está formada por 30 Estados, incluyendo la adhesión de España en 1982, dispuestos a respaldar los principios del tratado fundacional y velar por la seguridad de la Alianza.

Firma del Tratado de Washington en 1949. Source: Canal HISTORIA

ARTÍCULO V "DEFENSA COLECTIVA"

La OTAN opera en base a la premisa de "uno para todos, todos para uno". Este principio se encuentra reflejado en el artículo V del Tratado de Washington, el principio de "Defensa Colectiva":

"*Las partes convienen en que un ataque armado contra una o contra varias de ellas, acaecido en Europa o en América del Norte, se considerará como un ataque dirigido contra todas ellas y, en consecuencia, acuerdan que si tal ataque se produce, cada una de ellas, en ejercicio del derecho de legítima defensa individual o colectiva, reconocido por el artículo 51 de la Carta de las Naciones Unidas, asistirá a la Parte o Partes así atacadas, adoptando seguidamente, individualmente y de acuerdo con las otras Partes, las medidas que juzgue necesarias, incluso el empleo de la fuerza armada, para restablecer y mantener la seguridad en la región del Atlántico Norte*".

ARTICULO VI

El artículo V del Tratado se complementa con el artículo VI que estipula en qué situaciones un ataque será considerado "ataque armado contra una o varias de las Partes". El artículo hace referencia a los ataques dirigidos contra el territorio de cualquier Estado miembro de la Alianza, o bajo su jurisdicción; y contra sus Fuerzas Armadas:

"*Contra el territorio de cualquiera de las Partes en Europa o en América del Norte, contra los departamentos franceses de Argelia, contra el territorio de Turquía o contra las islas bajo la jurisdicción de cualquiera de las Partes en la zona del Atlántico Norte al norte del Trópico de Cáncer.*

Contra las fuerzas, buques o aeronaves de cualquiera de las Partes que se hallen en estos territorios, así como en cualquier otra región de Europa en la que estuvieran estacionadas fuerzas de ocupación de alguna de las Partes en la fecha de entrada en vigor del Tratado, o que se encuentren en el Mar Mediterráneo o en la región del Atlántico Norte al norte del Trópico de Cáncer".

COMPROMISO DEL ARTICULO V

Los Estados miembros de la OTAN se comprometen a garantizar la defensa colectiva de la Alianza a través de la asistencia y apoyo necesarios. La intervención de cada aliado se considera obligación y responsabilidad individual. Asimismo, es determinada por cada Estado en función de la coyuntura actual y las circunstancias particulares.

La respuesta no debe ser necesariamente militar. Se llevará a cabo de forma coordinada y en función de los recursos disponibles. Sin embargo, cada Estado se encargará de decidir su contribución teniendo en cuenta el objeto del artículo V "*restablecer y mantener la seguridad del espacio del Atlántico Norte*".

Hasta la fecha, el artículo V se ha invocado únicamente en una ocasión, en septiembre de 2001.

ATENTADOS DEL 11-S

Tras los atentados del 11 de septiembre de 2001 en el World Trade Center de Nueva York, Estados Unidos, perpetrados por la organización terrorista yihadista Al-Qaida, la esfera internacional tuvo que hacer frente a un evento que marcaría un punto de inflexión en la política de Seguridad Internacional.

Un atentado de tales magnitudes requería una respuesta eficaz y efectiva. Así, tras el estudio de los acontecimientos, la OTAN invocaba por primera vez en la historia la aplicación del artículo V de su tratado fundacional, la Defensa Colectiva.

Atentados del 11-S en Estados Unidos. Source: BBC

Con estas palabras, 24 horas después de la comisión de los atentados, se declaraba la autoría de Al Qaida y se categorizaba el atentado como un ataque armado contra la Alianza Atlántica:

"*Los hechos son claros y contundentes. La información presentada apunta de forma concluyente a un papel de Al-Qaida en los atentados del 11 de septiembre. Sabemos que los individuos que llevaron a cabo estos ataques formaban parte de la red terrorista mundial de Al-Qaida, dirigida por Osama bin Laden y sus principales lugartenientes y protegida por los talibanes*".

Desde su eclosión a nivel global, el fenómeno del terrorismo había sido categorizado por la OTAN como una amenaza a su seguridad. Sin embargo, la comisión de los atentados del 11-S y la expansión de la actividad terrorista supuso el compromiso de la Alianza con la lucha antiterrorista y el inicio de una campaña reactiva, promoviendo las primeras operaciones militares fuera de la zona euroatlántica y adaptando sus capacidades a las necesidades emergentes.

RESPUESTA COMÚN

La respuesta de la OTAN ante los ataques y su apoyo a Estados Unidos se tradujo en el lanzamiento de dos operaciones y la aprobación de un paquete de ocho medidas dirigido a combatir la amenaza terrorista.

La primera operación antiterrorista, conocida como Eagle Assist, se lanzó en el mes de octubre de 2001 y concluyó en mayo de 2002. Siete aviones de vigilancia AWACS de la OTAN fueron desplegados para patrullar el cielo de Estados Unidos. En total, se llevaron a cabo 360 vuelos.

El 26 de octubre de ese mismo año, se lanzó la segunda operación antiterrorista como respuesta a los atentados del 11-S.

La operación, conocida como *Active Endeavour* consistió en el despliegue de las Fuerzas Navales Permanentes de la OTAN para patrullar el Mediterráneo Oriental, vigilar la actividad marítima y disuadir la posible actividad terrorista en la zona. En marzo de 2004, el ámbito de aplicación se expandió por todo el Mar Mediterráneo.

En julio de 2015, el Consejo del Atlántico Norte aprobó la sustitución de la Active Endeavour por la Operación Sea Guardia, una misión "No Artículo 5" que continúa en la actualidad con la participación de España como Estado Miembro de la Alianza.

EL 11-S Y LAS OCHO MEDIDAD DE LA OTAN

Las ocho medidas implementadas por la Alianza Atlántica para dar respuesta a los ataques perpetrados por Al Qaida en Estados Unidos y hacer frente a la amenaza terrorista a nivel internacional fueron las siguientes:

1. Mejorar el intercambio de información y la cooperación, tanto bilateralmente como en los órganos apropiados de la OTAN, en relación con la amenaza terrorista y las medidas que deben adoptarse para combatirlo.
2. Proporcionar asistencia, individual o colectiva, a los Aliados y otros países que puedan ser objeto de amenazas terroristas como consecuencia de su apoyo a la lucha antiterrorista de la OTAN.
3. Adoptar medidas necesarias para garantizar la seguridad de las instalaciones de Estados Unidos y otros países aliados en su territorio.
4. Reforzar los recursos y medios de los países aliados necesarios para apoyar las operaciones de lucha contra el terrorismo.

5. Autorizar los sobrevuelos militares de los aviones de Estados Unidos y otros países aliados que se encuentren en el marco de operaciones antiterroristas, de conformidad con los acuerdos de tráfico aéreo y las normas nacionales.
6. Proporcionar el acceso a Estados Unidos y otros países aliados a los puertos y aeródromos nacionales de los Estados miembros de la OTAN para apoyar la lucha antiterrorista.
7. Compromiso de desplegar las Fuerzas Navales Permanentes de la OTAN por el Mediterráneo Oriental para disuadir y demostrar sus capacidades.
8. Compromiso de desplegar las Fuerzas Aéreas de Alerta Temprana de la OTAN para apoyar la lucha antiterrorista.

EVOLUCIÓN DE LA DEFENSA COLECTIVA

Desde la primera invocación de la Defensa Colectiva, los Estados miembros de la Alianza Atlántica han tenido que hacer frente de forma conjunta a la amenaza terrorista en sus diferentes formas y a otras amenazas para la seguridad internacional, desde el calentamiento global, pasando por el incremento de ciberataques hasta la pandemia mundial de la COVID-19.

Con el paso del tiempo, el tablero de juego internacional se ha caracterizado por un escenario cambiante y complejo con la intervención de diversos actores, estatales y no estatales; y la aparición de nuevas amenazas de carácter híbrido.

El compromiso de la OTAN para con sus Estados miembros se ha traducido en la respuesta a sus demandas y necesidades. Con respecto a la invocación del artículo V, la Alianza continúa desarrollando actividades y operaciones en el marco de sus actividades para garantizar la paz del espacio atlántico.

A petición de Turquía, miembro desde 1952, la OTAN ha puesto en marcha en diversas ocasiones medidas englobadas en el principio de Defensa Colectiva. Las más recientes fueron en 2003, con la aprobación de un paquete de medidas defensivas y disuasorias durante la crisis de Irak, conocido como la Operación Display Deterrence. En 2012, con el despliegue de sistemas de misiles Patriot en respuesta a la situación de crisis en Siria.

En la actualidad, España participa en la misión defensiva Active Fence de la OTAN cuyo principal objetivo es proteger a Turquía de posibles ataques con misiles balísticos procedentes de Siria.

En 2014, la anexión ilegal de Crimea por parte de Rusia y el aumento de la amenaza terrorista a nivel global protagonizado por organizaciones yihadistas como el Estado Islámico (Daesh) provocaron el mayor incremento de operaciones de Defensa Colectiva de la OTAN desde la Guerra Fría.

Entre las medidas llevadas a cabo, se ha triplicado la Fuerza de Respuesta de la OTAN; se han desplegado más de 5.000 efectivos como la punta de lanza de la Alianza; se han desplegado brigadas militares internacionales en Estonia, Letonia, Lituania y Rumanía; y se ha intensificado la vigilancia aérea sobre los Países Bálticos y el Mar Negro.

En 2016, los Estados miembros se reunieron en la Cumbre de Varsovia reconociendo, por primera vez en la historia, la ciberdefensa como un nuevo espacio operativo común para garantizar la seguridad del ciberespacio y el desarrollo de operaciones cibernéticas a través de la aportación de servicios y capacidades de los aliados.

A día de hoy, la OTAN garantiza la Defensa Colectiva, no solo como respuesta a peticiones o eventos puntuales, sino a través de Fuerzas Permanentes en servicio activo que contribuyen a los esfuerzos de la Alianza.

LAS FUERZAS PERMANENTES DE LA OTAN

Las Fuerzas Permanentes de la OTAN contribuyen de forma ininterrumpida a garantizar la seguridad del espacio atlántico. Entre ellas, se encuentran las fuerzas permanentes navales y aéreas, los sistemas de defensa integrados y el sistema de defensa contra misiles balísticos.

La Fuerza Naval Permanente de la OTAN desarrolla diferentes tareas, desde maniobras hasta misiones operativas, tanto en tiempos de crisis como en tiempos de paz. Las fuerzas aéreas llevan a cabo misiones de vigilancia que permiten a la OTAN detectar cualquier violación o infracción que se produzca en su espacio aéreo y tomar las medidas oportunas. Por otro lado, el sistema integrado de defensa aérea permite protegerse de posibles ataques aéreos y comprende el sistema de defensa contra misiles balísticos de la OTAN.

LA DEFENSA COLECTIVA 2.0

El concepto de Defensa Colectiva fue acuñado en 1949 respondiendo a los riesgos y desafíos de la época post Segunda Guerra Mundial con el objetivo de garantizar la seguridad ante un ataque armado contra los Estados miembros de la Alianza Atlántica y sus aliados.

La Defensa Colectiva ha permitido hacer frente a las amenazas y desafíos de carácter transnacional que han emergido a partir de la segunda mitad del siglo XX evolucionando a la par que las sociedades.

Sin embargo, la consolidación de las Nuevas Tecnologías de la Información y la Comunicación, los avances industriales y el impacto de amenazas internacionales híbridas han sacado a relucir la importancia de recategorizar el concepto de Defensa Colectiva y adaptarlo a un nuevo concepto de seguridad.

En pleno siglo XXI, la aparición de nuevos espacios comunes como el ciberespacio, la presencia de nuevos actores en el tablero de juego internacional y la creación de nuevas armas de destrucción químicas y biológicas plantean un escenario más complejo y la necesidad de redefinir los parámetros de un “ataque armado”.

Sin olvidar que muchas amenazas consideradas tradicionales o “del pasado” volverán en el futuro mutando y convergiendo con las contemporáneas. Quién se iba a imaginar que en el año 2020 la sociedad viviría una pandemia mundial que desembocaría en una de las crisis sanitarias más críticas de la historia. O que unos piratas robarían y secuestrarían barcos poniendo en riesgo la cadena de suministro de recursos de Europa.

Autora: Pino Penilla Marquínez. Analista de ciberinteligencia. Coordinadora del área de Defensa Nacional Sec2crime. Dirección Adjunta.

Análisis Robo de Mercancías Barcelona by Tapa

Resumen: El pasado Agosto 2020 la asociación TAPA (Transported Asset Protection Association) publicó en su revista Vigilant, el análisis realizado por Stephen Bacot y Kristian Bischoff, sobre el robo de mercancías en la Ciudad de Barcelona. En este artículo mostraremos algunos de sus resultados de las investigaciones realizadas y cómo está afectado el robo de mercancías a España.

PÉRDIDAS ECONÓMICAS EN CADENA DE SUMINISTRO

En 2019 la Comunidad Europea publicó la guía "EC Security Guidance for the European Commercial Road Freight Transport Sector", donde se exponen recomendaciones sobre las pautas a seguir para prevenir posibles robos durante toda la cadena de suministros.

Además, exponía que las pérdidas ocasionadas por robos durante la cadena de suministro ascienden aproximadamente a 8,2 € billones anuales, sin incluir los costes sociales (sistema judicial, investigación policial), operativos (sustitución de productos, cambios de planificación en la logística, costes administrativos, implantación de medidas de seguridad, ...) y a los seguros que generan este tipo de acciones delictivas, impactando tanto a empresas privadas como a las administraciones públicas.

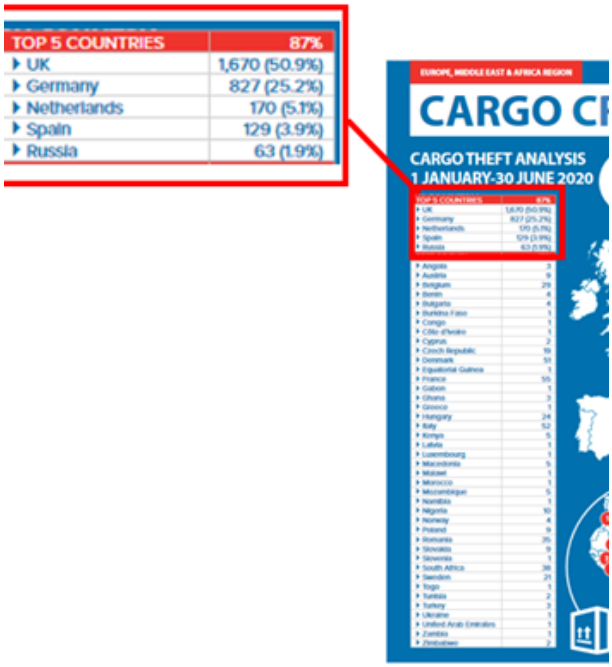
Asimismo, la asociación TAPA (Transported Asset Protection Association), en su revista mensual TAPA VIGILANT realiza un análisis mensual sobre los incidentes de seguridad reportados en su plataforma

TAPA VIGILANT

En la edición de agosto, publicó el reporte semestral (Enero a Junio 2020) sobre el *"Análisis de Robo de Mercancías"*, situando a España como uno de los cinco principales países de la Región de MLEMEA donde mayor robo de mercancías se produce (129 incidentes de seguridad, 3,9%)

En el mismo reporte expone cómo ha afectado las restricciones de movimiento durante el confinamiento, en el cual se ha observado que prácticamente habían sido erradicas y que los ladrones oportunistas habían optado por permanecer en casa, debido a la alta movilización de las Fuerzas y Cuerpos de Seguridad para dar apoyo a los protocolos de seguridad durante dicho periodo.

.



TOP 5 COUNTRIES	87%
UK	1,670 (50.9%)
Germany	827 (25.2%)
Netherlands	170 (5.1%)
Spain	129 (3.9%)
Russia	63 (1.9%)

Sin embargo, la llegada del COVID, también ha generado nuevas oportunidades delictivas como es la alta demanda de la sociedad hacia los productos de equipo de protección individual (EPIs) como mascarillas, gel hidroalcóholico,... Señalando como uno de los incidentes más graves el robo de 2 millones de mascarillas y otros EPIs por valor de 5 millones de euros en un almacén ubicado en Santiago de Compostela (Galicia)

Igualmente, en sus datos se muestra que el 18,2% (617 incidentes) afectan a las entregas de *Last Mile* poniendo su foco en esta entrega TAPA Vigilant, al análisis de robos de la última milla en Barcelona.

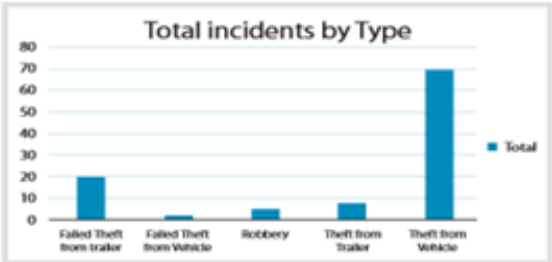
BARCELONA: PERFECTO LUGAR PARA ROBAR

Según el estudio publicado, Barcelona es considerada como una de las ciudades europeas más atractivas para los ladrones de mercancías en Europa y, en consecuencia, la más afectada por robos en España. Pero... ¿por qué elegir a la Ciudad Condal?

Bacot, S. y Bischoff K. (autores del reporte) exponen los siguientes factores por los que Barcelona se ha convertido en un área apetitosa para robar:

1. Es un objetivo con un rico entorno, tanto por su situación geográfica como por el peso económico de la logística en la región *(representa 13,9% del PIB catalán según la 15ª edición del Observatorio de la Logística)*
2. Su tráfico denso y sus calles estrechas generan numerosas oportunidades delictivas para identificar, seguir y/o emboscar a los vehículos de las entregas de Last mile.
3. Las áreas de servicio localizadas en los alrededores de la ciudad llegan a convertirse en objetivos principales de ciertas organizaciones criminales itinerantes.

Tactics used for all 105 cargo crimes in Barcelona in the past year



Types of incidents for all 105 cargo thefts in Barcelona in the past year

Sin embargo, lejos de poder plantear posibles soluciones para mitigar estas amenazas, el reporte expone que es una situación que va a prologarse durante mucho tiempo. Así pues, finaliza el reporte:

"En Barcelona, cada calle y lugar es una potencial parada de entrega, en consecuencia, se convierte en una posible escena del crimen. Los agentes amenazantes son demasiados numerosos, y los lugares donde suceden los incidentes de seguridad se encuentran demasiado dispersos para poder realizar una correcta monitorización e interceptarlas. Por ello, las empresas logísticas deben responder a través de sus propios procedimientos de seguridad y en la creación de herramientas de evaluación para la prevención de los robos".

¿LA CRIMINOLOGÍA PUEDE DAR ALGÚN SOPORTE A ESTA SITUACIÓN?

Si y mucho, como puede ser a través del estudio del entorno, la conocida CPTED (Crimen Prevention Through Environmental Design) o también denominada, la prevención de la delincuencia mediante el urbanismo.

No solo haciendo referencia a la iluminación de un parking o área de servicio, o a la disposición de las cámaras, sino también a tener en cuenta el número de salidas de esas áreas y la facilidad o rapidez de escapar de las mismas, así como posibles riesgos que se puedan crear debido a la alta demanda y como prevenirlos para evitar un incremento de los mismos (Black Friday, Navidades, ...)

Asimismo, la criminología puede dar soporte sobre la recomendable ubicación de los lockers de las estaciones de entrega como los Citypaq, Amazon Hub,... para prevenir posibles riesgos, creando un equilibrio entre la cercanía del consumidor final y su seguridad.
Todo ello a través de la investigación y de su posterior prevención.

Asimismo, la criminología puede dar soporte sobre la recomendable ubicación de los lockers de las estaciones de entrega como los Citypaq, Amazon Hub,... para prevenir posibles riesgos, creando un equilibrio entre la cercanía del consumidor final y su seguridad.

Todo ello a través de la investigación y de su posterior prevención.

Autora: Begoña Romero. Criminóloga especializada en Seguridad Corporativa. Colaboradora de Sec2Crime.

Los Mayores de 60 años: Un Colectivo Vulnerable para el Ciberfraude

Resumen: En artículos anteriores, como por ejemplo en el de Mirna Zárate en "Los fraudes en cheques; Un delito que sigue vigente en el siglo XXI . (sec2crime.com)" se puede ver uno de los diferentes métodos de fraude cibernético que existen. Sin embargo, desde que ha surgido la pandemia de Covid-19 éstos se han ido modificando y adaptando a las nuevas circunstancias sociales que vivimos.

En el año 2020, tal y como menciona el informe del FBI "Internet Crime Report 2020" en Estados Unidos se han denunciado 791.790 delitos cibernéticos. De todos ellos, el 13% de esas denuncias, es decir, 105.301 son de personas mayores de 60 años que han sido víctimas de algún tipo de fraude cibernético.

Y esta situación es perfectamente extrapolable a España, debido a que el colectivo de personas mayores de 60 años es uno de los puntos más débiles en la cadena de víctimas de fraude.

MÉTODOS:

Uno de los métodos más utilizados por los ciberdelincuentes sobre todo con este colectivo son las denominadas "llamadas telefónicas" o los "vishing". Éstas consisten en llamar a las víctimas dándoles en ocasiones los datos personales o solicitándoselos mientras se hacen pasar por la compañía de teléfono, el banco del cliente, compañías de electricidad, luz, agua, etc.

También pueden ofrecer descuentos en los contratos de suministro, o en el supuesto de que digan que están llamando del banco, pueden justificarse diciendo que se ha producido un cobro o varios en la cuenta bancaria de la víctima y que el motivo de la llamada es precisamente ayudarles para eliminar esas operaciones.

En el caso del vishing se pueden dar las mismas situaciones pero, a diferencia de la llamada telefónica simple, el ciberdelicuente pretende obtener los datos de la víctima dando excusas como por ejemplo: "*Buenos días, mi nombre es Pedro González y trabajo en la compañía encargada de la seguridad de su ordenador. Dejaremos de ofrecer nuestros servicios la próxima semana, con lo cual le ofrecemos un reembolso por 300 dólares. Por favor, comuníquese a este número de lunes a viernes en horario laboral...*"

Otro método que ha surgido a raíz de la pandemia del Covid19 ha sido el de utilizar la vacunación como excusa para obtener los datos personales de la víctima, tales como el nombre completo, la fecha de nacimiento y el hospital o centro sanitario donde recibió las dosis.

En el caso de personas mayores que llegan a utilizar internet, así como un correo electrónico, Whatsapp y otras aplicaciones online también son un blanco fácil. En este sentido podemos encontrar por ejemplo el "phishing". Éste se basa en, por ejemplo, recibir un correo electrónico donde se pueden incluir ofertas o promociones, o descuentos en compras, en contratos con nuevas compañías de suministro, o en su caso, pueden ser correos simulando ser del banco del cliente solicitando la actualización de los datos personales o simplemente ofreciendo nuevos productos.

También existen las "páginas espejo". Éstas se caracterizan porque son páginas idénticas a las originales, lo que hace que sea muy fácil confundirlas, pero a diferencia de las originales éstas pueden introducir virus o malware en los dispositivos y así obtener la información de los usuarios y poder gestionarla bajo sus propios intereses.

En ocasiones también pueden surgir fraudes a través de ofertas para unirse a colaborar en ONG's, ya sea de manera telefónica, vía internet, SMS o presencial.

Todos estos casos mencionados han sido con diferencia los métodos más utilizados en los últimos años, destacando así un total de 241.342 casos de phishing, vishing, smishing y pharming en 2020

CONSEJOS

En 2020 utilizaron internet un total de 32.8 millones de usuarios en todo el mundo, según el instituto nacional de estadística, donde un 70.5% utilizado es por hombres y un 68.9% es por mujeres, todos ellos mayores de 60 años en ambos casos. Sin embargo, es precisamente éste colectivo el que menor información tiene sobre este tipo de delitos.

Una primera medida podría ser la de impartir formación específica sobre ciberdelincuencia en centros de mayores o en lugares donde impartan clases para este tipo de colectivo.

También es importante dedicar un tiempo a nuestros mayores e informarles de las medidas que han de tomar para intentar evitar que les defrauden, es decir, usar la concienciación social. Por ejemplo, enseñarles a que si reciben una llamada para una encuesta que no den datos personales como el nombre completo, DNI, número de teléfono, etc.
En ocasiones también pueden recibir llamadas o visitas de personas que dicen ser revisores o representantes de la compañía de la luz, gas, agua, pero no llegan a mencionar claramente a qué compañía pertenecen ya que intentar saturar al cliente con mucha información y centrándose en la idea de que les van a aplicar descuentos, o les van a contratar otra tarifa más económica.

Y ocurre lo mismo cuando llaman haciéndose pasar por el banco del cliente. Hay que explicarles que estas empresas, no solicitan datos personales del cliente (tales como DNI, claves de acceso, clave de firma, etc) ya que ellos ya disponen de toda esta información en sus archivos internos.

En el caso de que sean ofertas o representantes de ONGs siempre es mejor acudir o llamar directamente a los teléfonos oficiales ofrecidos para ello, aunque obviamente, esto también se puede hacer en los otros casos anteriormente mencionados.

O si recibe una llamada para establecer una cita médica en casa cuando con anterioridad no se ha solicitado nada al centro de salud, ya que sino has solicitado una cita, o no estás a la espera de recibir alguna, los centros de salud y hospitales no llaman para citar a nadie.

CONCLUSIÓN:

Es cierto que hoy en día incluso las personas más jóvenes en muchas ocasiones no disponemos de toda la información necesaria para poder evitar este tipo de fraude, y que incluso muchas veces, aunque se tenga la información es difícil poder evitarlo, sin embargo, es importante no olvidarnos de nuestros mayores ya que al final son uno de los colectivos más sensibles y vulnerables ante este tipo de delitos.

Por lo tanto, no solo hay que intentar prevenir el ciberfraude en todas sus formas, sino que también es importante que la información necesaria para ello llegue a todos los rincones del mundo.

Autora: Verónica Pérez. Analista de prevención del fraude y PBC. Coordinadora y colaborado del área de prevención de blanqueo de capitales de Sec2crime

Seguridad en las Carreteras

Resumen: España es uno de los países con mayor concienciación entre sus ciudadanos en relación con la seguridad vial. Constantemente encontramos campañas de publicidad presentadas por el Ministerio del Interior en distintos medios de comunicación. ¿Cómo ha evolucionado la seguridad en carreteras? La criminología vial contiene algunas de las respuestas para reducir el riesgo de accidentes de tráfico.

INTRODUCCIÓN

Los accidentes de tráfico son un problema global que hay que solventar. Las defunciones constan como la octava causa mundial de muerte, sobre todo para gente joven. La evolución de las sociedades, en constante cambio, han provocado que se crean nuevas necesidades entre los ciudadanos; y entre ellos se encuentra el desplazamiento por carretera.

En 1900 se aprobó en España el Reglamento para el Servicio de Coches Automóviles por las diferentes Carreteras del Estado. En él se incluía las necesidades básicas con las que debía contar el automóvil si quería circular por carreteras: bocina, faroles, indicadores lumínicos y dos sistemas de freno. Además de limitar la velocidad según las distintas vías.

En relación con la regulación de las señales de tráfico, no llegaría a España hasta 1968. Se realizó en la convención de Viena, participando 65 países de diferentes continentes para unificar los diseños de dichas señales.

Durante la primera década del siglo XXI, España tomó medidas urgentes para reducir las tasas de accidentes en sus vías. Los resultados mostraron que los siniestros se redujeron hasta un 31%. Los países que lo siguieron fueron los Estados Unidos y dentro de los europeos, Francia y Suecia.

El pasado año, la pandemia provocó restricciones de movilidad y entre ellos también se incluía en las carreteras. Aun así, la Dirección General de Tráfico (DGT), afirmó que este mismo hecho provocó que los pocos conductores que se encontraban en las vías se sintieran más relajados e infringieran algunas de las normativas viales, como no abrocharse correctamente el cinturón o exceder el límite de velocidad.

Este año 2021, el Ministerio del Interior ha presentado la nueva campaña elaborada por la Dirección General de Tráfico que vela por la seguridad en los desplazamientos y por la concienciación del uso correcto de comportamiento al volante.

SEGURIDAD VIAL EN EL MUNDO

La Unión Europea continúa empleando medidas para seguir reduciendo los accidentes de tráfico, clasificándose como el continente con mayor nivel de seguridad vial. España se sitúa en cuarta posición, y por delante, Suecia, Malta y Dinamarca.

Además de ello también han propuesto una Iniciativa de Movilidad Urbana Transformativa. Consiste en que países de la Unión Europea desarrollen sistemas de transporte urbano seguros y adaptados a las grandes ciudades.

Fuera del continente europeo, **América del Sur** pretende tomar las mismas medidas, pero carece de recursos tales como un sistema efectivo de recogida de datos, una institución consolidada, auditorías constantes, entre otros, que dificultan que se cumplan los objetivos planteados. En cambio, en **Norteamérica**, el National Highway Traffic Safety Administration (NHTSA) es quien se ocupa de reducir el número de muertos y lesionados por accidentes de tráfico.

Dentro del continente asiático, el pasado año 2020 empezó a estar disponible la web del Observatorio de Seguridad Vial, concretamente en **Asia Pacífico** (APRSO). Se trata de un foro regional donde constan las políticas, los datos y las prácticas de seguridad vial para poder garantizar la protección en carreteras de los usuarios. Para ello contó con el apoyo de numerosas organizaciones, como el Foro Internacional de Transportes, la Federación Internacional de Automovilismo (FIA), así como el Banco Mundial o el Banco Asiático del Desarrollo.

En el continente africano, la Federación Internacional de Automovilismo (FIA), junto a la Fundación Prudence y la Fundación Didier Drogba se unieron para crear la campaña SAFE STEPS Road Safety África.

Se trata de un programa que hace uso de varias plataformas para concienciar a los usuarios de carreteras proporcionando información clara y simple. El motivo principal es que África tiene altas tasas de mortalidad comparadas con el resto del mundo. Con la campaña se pretende reducir riesgos y que los usuarios respeten las reglas básicas de seguridad vial.

Se trata de un programa que hace uso de varias plataformas para concienciar a los usuarios de carreteras proporcionando información clara y simple. El motivo principal es que África tiene altas tasas de mortalidad comparadas con el resto del mundo. Con la campaña se pretende reducir riesgos y que los usuarios respeten las reglas básicas de seguridad vial.

Finalmente en Oceanía, donde principalmente Australia toma iniciativas en relación con impacto que tiene en las víctimas los accidentes de tránsito y en la creación de cortinas de agua convertidas en señal de tráfico (Softstop Barrier System) que ayudan a los conductores a tener mayor visión en la calzada.

El objetivo principal del mismo es que impacte visualmente para reducir el riesgo de accidente. Todo ello gracias al International Road Assessment Programme (iRAP), quien se encarga de llevar a cabo estudios sobre la seguridad en las carreteras.

PRINCIPALES VÍCTIMAS

Los mayores perjudicados en los accidentes de tráfico son los usuarios de la vía pública, tales como los peatones, ciclistas y motociclistas. Todos ellos representan casi la mitad de las víctimas mortales.

Según un estudio del Global Status Report on Road Safety (GSRRS), el 90% de accidentes de tráfico con víctimas mortales, se encuentran países con bajos ingresos y medianos. De todos ellos, el 62% se producen en países con mayor magnitud, como India, China, Estados Unidos, Rusia o Brasil.

En **territorio español**, el 75% de muertos en carreteras fueron dentro de las convencionales.

El 46% fueron salidas de vía, el 27% por altas tasas de alcohol en sangre y el 33% por distracciones como el uso del teléfono móvil.

CRIMINOLOGÍA VIAL

¿Qué papel guarda la criminología dentro de la seguridad en carreteras? La criminología vial es la especialización encargada de velar por la seguridad y reducir los riesgos de accidentes de tráfico.

Los criminólogos distinguimos siniestros de accidentes. Los primeros estarían relacionados con una situación donde los conductores no pueden controlar el entorno, como sería el estado de la vía, mientras que en los siniestros sí, un exceso de velocidad.

Quienes trabajan dentro de esta área se encargan de analizar el comportamiento de los conductores, peatones y resto de víctimas para así tratar de evitar riesgos y aportar soluciones a los delitos que se producen.

Después de recopilar y analizar los datos, para los criminólogos nos es más fácil tomar medidas preventivas. Crear políticas públicas que cambien el diseño de intervenciones, así como tener en cuenta el entorno donde los accidentes se producen.

Para ello se hace uso de mapas del crimen, donde se van anotando los lugares donde existe un mayor riesgo o se cometen las infracciones.

Por tanto, el objetivo principal es intervenir en la siniestralidad vial desde una perspectiva criminológica, preventiva, como de las víctimas y los conductores.

Por tanto, el objetivo principal es intervenir en la siniestralidad vial desde una perspectiva criminológica, preventiva, como de las víctimas y los conductores.

En Sec2Crime tenéis disponible el artículo de mi compañera Kateryna Andriana Ivashkiv, “Modus operandi: el método pincha-ruedas”, donde explica un mecanismo creado para extraer objetos valiosos del interior de vehículo sin que se percate el conductor o conductora. Os animo a que cliquéis en el enlace y descubráis más sobre ello.

Autor: Anaïs Iglesias Pérez. Criminóloga y Colaboradora de Sec2Crime.

La Lucha Antiterrorista vista por la Plana Política: qué está bien y qué es mejorable

Resumen: *España lleva sufriendo el terrorismo, a intervalos intermitentes, más de cinco décadas. Desde los Grapo y el FRAP hasta la banda terrorista más sanguinaria, ETA, que asesinó a 854 personas desde su primer asesinato en 1968 hasta el año 2010. El terrorismo de corte yihadista también ha hecho mella en nuestro país; en 1985 con el atentado en el restaurante El Descanso, que dejó 18 muertos; el 11 de marzo de 2004, cuando diez bombas explosionaron casi de forma simultánea en varios puntos de la red de Cercanías de Madrid, dejando 192 muertos; y el 17 de agosto de 2017, cuando tuvo lugar un atropello masivo en Las Ramblas de Barcelona, que acabó con la vida de 16 personas. Las nuevas tecnologías, la pandemia de la COVID-19 o el peligroso avance de nuevas formas de hacer terrorismo, hacen que sea primordial contar con medidas eficientes para luchar contra este fenómeno, y, para ello, es necesario conocer las intenciones de los partidos políticos en cuanto a medidas de seguridad y prevención de la radicalización.*

INTRODUCCIÓN

España siempre ha actuado de catalizador del tiempo en todos los atentados que ha sufrido; el tiempo parecía detenerse durante unos instantes para proseguir con el correteo de ambulancias y policías aplazando las preguntas y los porqués de aquellos desastres. El país entero se ha visto magullado por un terror sobrecogedor. ¿Y ahora ¿Seguimos estando expuestos a ese terror?

El matemático y físico Blaise Pascal dijo una vez que es más fácil soportar la muerte sin pensar en ella, que soportar el pensamiento de la muerte; y en parte, tenía razón. Es importante no dejar de vivir nuestras costumbres, es imprescindible no rendirnos a la espada del terrorismo ni doblegarnos ante aquellos que se hacen llamar soldados sin tener conocimiento de lo que significa serlo.

Pero esto no puede derivar en un olvido sistemático del peligro; la amenaza sigue existiendo, y hay que trabajar para frenarla.

Por ello, diferentes portavoces de los principales grupos parlamentarios en la Comisión de Interior han expuesto sus puntos de vista en cuanto a las medidas que impondrían para prevenir la radicalización violenta y luchar contra el terrorismo.

Antes de comenzar, es necesario aclarar un punto. Tras varios intentos de contacto con el Grupo parlamentario de Unidas Podemos, ha sido imposible realizar entrevistas, ni telefónicas ni presenciales, por no obtener contestación alguna por parte del partido. Por ello, se han extraído de su programa electoral las principales ideas sobre lucha antiterrorista.*

Para que sirva como enclave principal de este análisis, se nombrará a continuación la legislación actual de España en materia de terrorismo. Para empezar, la Ley Orgánica 1/2015 del 30 de marzo, afirma que será considerado delito terrorista "la comisión de cualquier delito grave contra la vida o la integridad física, la libertad, la integridad moral, la libertad e indemnidad sexuales, el patrimonio, los recursos naturales o el medio ambiente, la salud pública, de riesgo catastrófico, incendio, contra la Corona, de atentado y tenencia, tráfico y depósito de armas, municiones o explosivos, previstos en el presente Código, y el apoderamiento de aeronaves, buques u otros medios de transporte colectivo o de mercancías, cuando se llevaran a cabo con cualquiera de las siguientes finalidades:

1. Subvertir el orden constitucional, o suprimir o desestabilizar gravemente el funcionamiento de las instituciones políticas o de las estructuras económicas o sociales del Estado, u obligar a los poderes públicos a realizar un acto o a abstenerse de hacerlo.

2. Alterar gravemente la paz pública.
3. Desestabilizar gravemente el funcionamiento de una organización internacional.
4. Provocar un estado de terror en la población o en una parte de ella".

Además, en el año 2015, se aprobó la prisión permanente revisable, que consiste en una pena privativa de libertad con posible revisión de la condena cuando se haya cumplido una parte relevante de la pena. Según el Código Penal, es aplicable a delitos especialmente graves como delitos de lesa humanidad, asesinato de un jefe de Estado, asesinato terrorista, asesinato de una persona menor de 16 años o el asesinato tras cometer un delito contra la libertad sexual.

Esta última norma ha sido criticada por partido políticos como Unidas Podemos, Partido Nacionalista Vasco (PNV), Esquerra Republicana de Catalunya (ERC), Partido Demócrata Europeo Catalán (PdeCat) o EH Bildu.

En cuanto a la radicalización violenta, España cuenta con un Plan Estratégico Nacional cuyo objetivo es la detección temprana de focos de radicalismo violento.

Para ello, el Plan establece como coordinador al Ministerio de Asuntos Exteriores, y como actores principales a los Cuerpos y Fuerzas de Seguridad del Estado. También da relevancia a la secretaria general de Instituciones Penitenciarias, para que elabore informes sobre la situación de la radicalización violenta en las cárceles.

En el área de la lucha contra el terrorismo y la radicalización violenta, los grandes grupos parlamentarios, exceptuando a Unidas Podemos, han participado en este análisis a través de entrevistas en las que se ha hablado sobre la actual legislación, qué se debería cambiar y qué propuestas tiene cada partido.

Comenzaremos por el Partido Socialista Obrero Español (PSOE), a través de David Serrada, su portavoz en la Comisión de Interior del Congreso de los Diputados.

DAVID SERRADA (PSOE)

David Serrada afirma que la valoración en general de las medidas sobre seguridad y prevención del terrorismo que tiene el actual Gobierno de España es correcta. Se da importancia a la prevención de la radicalización violenta en las prisiones, así como a la investigación que llevan a cabo las Fuerzas y Cuerpos de Seguridad del Estado. Sobre la estipulación de penas privativas de libertad para delitos relacionados con el terrorismo, el Grupo Parlamentario Socialista afirma que a la espera de que el Tribunal Constitucional se pronuncie sobre la prisión permanente revisable, la intención es continuar con lo recogido en el Código Penal. (El pasado 06/10/21 el TC avaló por mayoría la prisión permanente revisable, rechazando los recursos de inconstitucionalidad que interpuso el PSOE junto con otros grupos parlamentarios contra la ley. Tras conocer el contenido de la resolución del Constitucional, la ministra de Justicia, Pilar Llop, ha descartado "reabrir el debate" puesto que el TC "ha hablado").

¿Cuál es la valoración del PSOE sobre el actual plan de medidas de seguridad que tienen el Gobierno de España?

La valoración que hacemos es positiva. El Gobierno de España ha puesto en marcha políticas que nosotros veníamos demandando desde nuestra época en la oposición, fundamentalmente en lo relativo a políticas preventivas y procesos de radicalización.

Sobre la estipulación de penas privativas de libertad, el PSOE está de acuerdo con la prisión permanente revisable para casos de terrorismo.

En materia de prevención de la radicalización violenta, ¿cuáles son las propuestas del partido?

En esta área se han sentado tres pilares importantes con los planes concretos. El primero serían los protocolos específicos en política penitenciaria que vienen desde el año 2018, pero que era necesario actualizar y se van a poner en práctica en lo que queda de año 2021. El segundo sería el trabajo que han venido realizando las Fuerzas y Cuerpos de Seguridad en su labor de investigación y de prevención, que están también contempladas en la Estrategia Nacional contra el terrorismo de colaboración o de establecer canales de colaboración tanto con policías locales como con la seguridad privada.

Y el tercer pilar de esta estrategia preventiva, que es fundamental, son las asociaciones y organizaciones de la sociedad civil. Y en este sentido es importante que aquellos colectivos que están en contacto directo en el día a día, conviviendo con los ciudadanos, puedan tener sus mecanismos y conozcan los protocolos que existen y que están a disposición de estas asociaciones para que puedan trasladar información a las Fuerzas y Cuerpos de Seguridad.

¿Qué cambios o nuevas medidas incluirían ustedes en el área de la lucha contra el terrorismo, a nivel de seguridad y prevención?

Las medidas estipuladas ahora fundamentalmente tienen que ver con cómo se detectan las amenazas y cómo se trabajan en un nivel de seguridad cuatro como el que estamos. Y ahí la labor del Centro de Inteligencia contra el Terrorismo y el Crimen Organizado (CITCO) es fundamental. Este organismo recibe la información de estas amenazas, y la distribuye y gestiona a través de los diferentes cuerpos de seguridad.

Hay algo importante que ha ocurrido en este periodo de pandemia, y es que durante la cuarentena esta labor no se ha parado.

¿Les parece correcta la estipulación de penas de prisión que tiene la legislación actual para delitos relacionados con el terrorismo o propondrían cambios?

A la espera de que el Tribunal Constitucional se pronuncie sobre la prisión permanente revisable, la intención es continuar con lo recogido en el Código Penal. Lo que estamos haciendo, desde el PSOE y desde el Gobierno de España, es seguir el marco conjunto que está estableciendo la Unión Europea.

España es uno de los países que, en política penitenciaria, en política antiterrorista y en cuestiones legislativas contra el terrorismo, es de los que más avanzados están, pero eso también nos da una idea del nivel de protección y de garantías jurídica que tenemos en España.

David Serrada.

TERESA JIMENEZ - BECERRIL (PP)

El Grupo Parlamentario Popular, a través de Teresa Jiménez-Becerril, miembro de la Comisión de Interior del Congreso de los Diputados, aunque ven correcta la adecuación de las medidas de seguridad y prevención al entorno europeo, hay determinadas acciones que no ven correctas y tachan de indignas, por ejemplo, los pasillos que se les hace a los etarras o que el Gobierno de la nación haya pactado con un partido que no condena en terrorismo (refiriéndose a Bildu). Ven importante la educación como canal para prevenir la radicalización violenta y en cuanto a la prisión permanente revisable en este tipo de delitos, el PP está de acuerdo con ella, ya que considera que esto da seguridad a las víctimas.

¿Cuál es la valoración del PP sobre el actual plan de medidas de seguridad que tienen el Gobierno de España?

Creo que respecto a combatir el terrorismo hay bastante unidad, empezando por el Pacto Antiterrorista. La mayoría de las medidas para luchar contra el terrorismo están enfocadas a nivel europeo porque es una amenaza global, y por tanto la respuesta ha de ser global.

Ahora bien, hay algunas diferencias entre nuestro país y Europa respecto a este tema, por ejemplo, en la respuesta a las víctimas. Hay un enfrentamiento con las víctimas del terrorismo, muchas de ellas víctimas de ETA, por la manera en que el Gobierno ha hecho los acercamientos de los terroristas, además del pacto con un partido que no condena el terrorismo.

Desde el PP tampoco vimos con buenos ojos que el presidente pusiera a su exvicepresidente primero, Pablo Iglesias, en el CNI, ya que considerábamos que no estaba ni preparado ni era la persona adecuada para estar ahí, con lo cual consideramos que eso fue un uso político y muy nocivo, que no respondía a criterios profesionales de ningún tipo.

En materia de prevención de la radicalización violenta, ¿cuáles son las propuestas del PP?

Desde el Partido Popular creemos que lo más importante es la prevención y la respuesta a las víctimas. Trabajamos para que esta prevención se haga desde todos los niveles educativos, además de programas en las prisiones para evitar radicalismos violentos, ya que es dónde existe un mayor potencial de radicalización.

También es importante diferenciar entre inmigración y terrorismo; no tienen nada que ver. Pero tampoco hay que ser ingenuo, ya que los terroristas buscan y buscarán cualquier canal para entrar en los países en los que pretenden atentar, y uno de esos canales es la inmigración. Creemos que es muy importante el control de fronteras, principalmente porque España está situada muy cerca de puntos calientes de inmigración.

Consideramos necesaria la cooperación de la Agencia Europea de la Guardia de Fronteras y Costas (Frontex), ya que es vital vigilar el tema de los retornado que vuelven después de haber luchado en las filas de organizaciones terroristas.

Desgraciadamente lo que pasa con el terrorismo es que, cuando hay atentados, suben mucho los niveles de alerta y enseguida se toman muchas medidas, pero en cuando la onda emocional que supone un ataque terrorista se dispersa, volvemos a no estar pendientes.

¿Qué cambios o nuevas medidas incluirían ustedes en el área de la lucha contra el terrorismo, a nivel de seguridad y prevención?

En materia de prevención la estrategia tiene que ser prevenir, proteger, perseguir, enjuiciar y dar respuesta a las víctimas. Se han de seguir todas las directrices europeas; no podemos estar divididos porque perjudicaría muchísimo a la sociedad.

¿Les parece correcta la estipulación de penas de prisión que tiene la legislación actual para delitos relacionados con el terrorismo o propondrían cambios?

El Grupo Popular está de acuerdo con la prisión permanente revisable, que al contrario de lo que se suele pensar, no es una cadena perpetua; es revisable. Creemos que los años que los jueces establezcan han de cumplirse íntegramente, para dar seguridad a las víctimas, además de para hacer justicia.

Hay que proteger la dignidad de los afectados. Por ejemplo, el terrorista de Juana Chaos escribía cartas desde la cárcel diciendo que nuestro llanto era su sonrisa; esto tampoco se puede permitir. Cualquiera pudo haber sido víctima y es el Estado quien debe procurar la justicia.

Por último, hay acciones que no deberían repetirse, como cuando hacen pasillos a los etarras. No me imagino a ningún líder político de ningún país haciendo pasillos a terroristas. ¿Por qué hay que aguantar que esta gente sea moneda de cambio para cuestiones políticas?

Teresa Jiménez-Becerril.

MIGUEL GUTIERREZ (Ciudadanos)

Desde el Grupo Parlamentario de Ciudadanos, Miguel Gutiérrez, portavoz de la Comisión de Interior, reclaman al Gobierno una mejor dotación de recursos para las Fuerzas y Cuerpos de Seguridad, ya que son ellos los que están en primera línea para evitar atentados. Proponen varias medidas, como la creación de un Observatorio de Terrorismo que estudio el fenómeno de la radicalización violenta. Sobre las sanciones para delitos que tengan relación con el terrorismo, Ciudadanos apoya la prisión permanente revisable.

¿Cuál es la valoración del Ciudadanos sobre el actual plan de medidas de seguridad que tienen el Gobierno de España?

España es un país modelo en cuanto a medidas de seguridad, pero aún falta por mejorar. Es insuficiente, hay que estudiar los fenómenos que empujan a las personas a radicalizarse y a cometer atentados.

En materia de prevención de la radicalización violenta, ¿cuáles son las propuestas del partido?

Yo creo que España, de hecho, es un ejemplo porque no ha habido mayor radicalización violenta que la que supuso el terrorismo ETA. Y a ETA se la combatió con la ley, y también gracias a la sociedad, por supuesto, pero sobre todo con la ley.

Hoy en día nos encontramos otros fenómenos de radicalización violenta también, como puede ser el terrorismo yihadista, pero también otro terrorismo de baja intensidad. Para saber cómo atajar este problema, desde Ciudadanos creemos hace falta un observatorio permanente donde, en base a expertos que sean convocados, haya un estudio permanente sobre por qué se produce esa radicalización violenta.

Existen dos líneas básicas de teoría del porqué ocurre, unos dicen que hay unos procesos por los que va pasando una persona que se va al radicalizando poco a poco hasta que acaba cometiendo un atentado; otros dicen que el que es violento es violento, no necesita ningún proceso para convertirse en violento y por tanto, el acercamiento a la prevención es distinto, por ello es importante el estudio del fenómeno.

También es vital la educación, desde el principio, para evitar no sólo radicalismos violentos sino también ideas como la relación entre la religión musulmana y el terrorismo. Muchas veces confunde a la gente.

¿Qué cambios o nuevas medidas incluirían ustedes en el área de la lucha contra el terrorismo, a nivel de seguridad y prevención?

Además del Observatorio que he mencionado antes, tenemos que apoyar a nuestras Fuerzas y Cuerpos de Seguridad, dotarles de más y mejores medios, que eso sí que es una opción de gobierno que nosotros reclamamos de forma continua. Al final son ellos los que están previniendo que se produzca un atentado.

¿Les parece correcta la estipulación de penas de prisión que tiene la legislación actual para delitos relacionados con el terrorismo o propondrían cambios?

La prisión permanente revisable nos parece correcta cuando se aplica por delitos con especial singularidad que supongan un dolo grave para la sociedad. La finalidad de las sanciones es trabajar en la reinserción, es algo que también hay que estudiar; es decir, es necesario saber si estas personas pueden o no reinsertarse en la sociedad. Si no se puede reinsertar, la prisión debe ser permanente.

¿Les parece correcta la estipulación de penas de prisión que tiene la legislación actual para delitos relacionados con el terrorismo o propondrían cambios?

La prisión permanente revisable nos parece correcta cuando se aplica por delitos con especial singularidad que supongan un dolo grave para la sociedad. La finalidad de las sanciones es trabajar en la reinserción, es algo que también hay que estudiar; es decir, es necesario saber si estas personas pueden o no reinsertarse en la sociedad. Si no se puede reinsertar, la prisión debe ser permanente.

Miguel Gutiérrez.

Macarena Olona (Vox)

Desde el Grupo Parlamentario de VOX, a través de su portavoz en la Comisión de Interior, Macarena Olona, ven insuficientes las medidas de seguridad para la lucha contra el terrorismo que tiene el Gobierno actual y le instan a tomar medidas concretas para evitar ataques a España. Entre ellas están las de cooperación internacional y reconocimiento de fronteras. En cuanto a las penas privativas de libertad, Vox está de acuerdo, aunque añade que son necesarias otras sanciones, como la pérdida de la nacionalidad española obtenida por adquisición derivativa (es decir a quien no sea español de origen) cuando haya sido condenado por delitos de terrorismo.

¿Cuál es la valoración de VOX sobre el actual plan de medidas de seguridad que tienen el Gobierno de España?

Las consideramos absolutamente deficientes. Por la situación geográfica de España, somos la puerta de acceso a Europa de todo el continente africano y con ello, uno de los principales problemas que sufre España es el de la entrada de terroristas yihadistas a través de la inmigración ilegal, por ello consideramos absolutamente necesario que el Gobierno tome conciencia de la amenaza que supone para la sociedad española unos flujos migratorios descontrolados, instigados y favorecidos por grandes redes del crimen organizado, que en multitud de ocasiones forman simbiosis con grupos terroristas. Una realidad que se ha negado en el Congreso de los Diputados, en la Comisión de Seguridad Nacional, por parte del resto de formaciones políticas cuando, en las iniciativas que ha promovido VOX basándose en la evidencia policial y judicial de la entrada de yihadistas a través de los flujos migratorios ilegales, se ha negado dicha evidencia y se nos ha calificado de racistas.

VOX propone que, en virtud de los artículos 23 y 24 de la Ley 36/2015, de 28 de septiembre de Seguridad Nacional, debe declararse la invasión migratoria que sufre España como situación de interés para la Seguridad Nacional y se deberá incluir el despliegue de todos los recursos humanos y materiales necesarios y suficientes (art.24.1 apartado E), en aras a la prevención, protección y disuasión de atraque de embarcaciones con inmigrantes ilegales.

En materia de prevención de la radicalización violenta, ¿cuáles son las propuestas del partido?

En el programa de las 100 medidas de VOX tenemos iniciativas en materia de prevención de la radicalización, entre las cuales se encuentran:

- El cierre de mezquitas fundamentalistas y expulsión de los imanes que propaguen el integrismo, el menosprecio a la mujer, o la yihad.
- Rechazar e ilegalizar la financiación por parte de terceros países de lugares de culto en suelo español.
- Exigir a los responsables de la religión islámica en España una absoluta colaboración para la detección de radicales y la exclusión de la enseñanza del islam en la escuela pública.
- Fortalecer nuestras fronteras: Levantar un muro infranqueable en Ceuta y Melilla y dar a policías y FFAA todos los recursos materiales y humanos para que puedan cuidar nuestras fronteras con total eficacia, junto con el amparo legal correspondiente.

- Incrementar y racionalizar el presupuesto de Defensa.
- Exigir a Marruecos un total reconocimiento y respeto de la soberanía española de Ceuta y Melilla.
- Publicación de datos sobre nacionalidad y origen en estadísticas de delitos.
- España participará en misiones militares de combate contra la amenaza yihadista de acuerdo a nuestros intereses y capacidades.
- Suspender espacio Schengen hasta que exista la garantía europea de que no lo utilizarán los criminales para huir de la justicia (como han hecho los golpistas separatistas) ni lo aprovechen las mafias de la inmigración ilegal para introducir personas.

¿Qué cambios o nuevas medidas incluirían ustedes en el área de la lucha contra el terrorismo, a nivel de seguridad y prevención?

Son múltiples las iniciativas que nosotros hemos presentado en el Congreso aportando cambios y nuevas medidas para prevenir y combatir el terrorismo.

Entre ellas hemos registrado una PNL en la Comisión de Seguridad Nacional el 3 de diciembre de 2020 para aumentar e incentivar los controles fronterizos nacionales y comunitarios, respectivamente, así como optimizar la coordinación entre las Fuerzas y Cuerpos de Seguridad del Estado como medidas de prevención y lucha contra el terrorismo infiltrado como inmigración irregular.

De igual manera, con fines de prevención y de seguridad para luchar contra el terrorismo, hemos registrado en el Congreso de los diputados, numerosas PNLS en aras a adoptar medidas en materia de inmigración ilegal. Entre ellas, una PNL registrada en la Comisión de Seguridad Nacional el 27 de noviembre de 2020, sobre la adopción de contramedidas de carácter urgente con el objeto de frenar la oleada masiva de inmigración ilegal hacia nuestras costas.

Entre las medidas que solicitábamos y que consideramos claves, para prevenir el terrorismo internacional están:

- Suspender la expedición de visados europeos a ciudadanos de países emisores de inmigración ilegal si estos no readmiten en sus fronteras a aquellos inmigrantes irregulares que dejan salir de sus costas.
- Denunciar ante organismos internacionales la agresión que sufre España por parte de los Estados del Norte de África al no controlar la inmigración ilegal.

Macarena Olona.

Otra PNL registrada el 5 de marzo de 2021 en la Comisión Mixta de Seguridad Nacional relativa a promover todas las acciones necesarias con la finalidad de dotar de los medios, recursos y efectivos suficientes y adecuados a las FCSE desplegados en las Islas Canarias, con el objeto de evitar y prevenir la infiltración de yihadistas a través de los flujos masivos de inmigración ilegal al archipiélago canario. Consideramos esencial que a nuestras FCSE se les dote de todos los medios materiales y humanos necesarios para combatir la inmigración ilegal y luchar contra el terrorismo.

Pero la lucha antiterrorista no se limita al terrorismo yihadista, sino que el Grupo Parlamentario de VOX es consciente del indudable incremento exponencial del terrorismo llevado a cabo por parte de la extrema izquierda y como tal registró una PNL el día 3 de julio de 2020 en el Congreso de los Diputados, en la que se instaba al Gobierno a desarrollar un protocolo de acción y seguridad ante el peligro generado por el aumento de dicha clase de terrorismo.

¿Les parece correcta la estipulación de penas de prisión que tiene la legislación actual para delitos relacionados con el terrorismo o propondrían cambios?

Parece correcta la estipulación de penas de prisión que llevan aparejados los delitos de terrorismo, pero no suficientes, pues la comisión de un delito de terrorismo debe de llevar aparejadas otras consecuencias, que deben de reflejarse en la pena impuesta, junto con la pena de prisión.

Y en este sentido, el Grupo Parlamentario de VOX, el 23 de marzo de 2021, registró una PNL ante el Pleno del Congreso de los Diputados por el que se instaba al Gobierno a acometer una reforma del Código Penal por la que se introduzca la pérdida de la nacionalidad española obtenida por adquisición derivativa, es decir, cuando no se sea español de origen, cuando haya sido condenado por delitos de terrorismo, delitos graves contra el orden público o cometidos en el seno de organizaciones criminales, pues la comisión de alguno de esos delitos implica una ruptura del vínculo del individuo con el Estado del que haya obtenido la nacionalidad, pues pone en riesgo la protección del Estado y de todos sus nacionales.

Y, en este sentido, debe primar la seguridad y protección del Estado y sus nacionales frente a la conservación de la nacionalidad de un español que la ha adquirido de forma derivativa.

***Unidas Podemos:** En su programa electoral se pueden encontrar únicamente dos puntos que hacen referencia a la lucha contra el terrorismo.

Punto 44. Una Europa segura desde un enfoque de derechos. Se impulsará la cooperación policial y judicial en la lucha contra el terrorismo y el crimen organizado transnacional —en particular, en la persecución del fraude y la corrupción—, logrando una mayor implicación de Eurojust y Europol. Se implementarán mecanismos para cortar las fuentes de ingresos extranjeros de la delincuencia transnacional y para perseguir su financiación oculta. Como se señaló en el Plan Europeo Contra la Corrupción, la UE establecerá un cuerpo de policía especializado en delitos de corrupción y delitos financieros que actuará a las órdenes del Poder Judicial de los Estados, al mismo tiempo que se fortalecerán las Unidades de Inteligencia Financiera en los propios Estados.

Punto 145. Plan Integral contra el Terrorismo Internacional. Se planteará un abordaje integral del fenómeno que dé respuesta también a las causas sobre las que los grupos terroristas expanden su barbarismo: la exclusión, las desigualdades, la difusión de la cultura del odio, la intolerancia, los fundamentalismos religiosos, así como sus fuentes de financiación y su acceso a las armas. En paralelo, se establecerán mecanismos que mejoren la cooperación policial, judicial y de los servicios de inteligencia, y el intercambio de información a escala europea y entre los Estados miembros, y se adoptarán políticas de seguridad y prevención basadas en la evidencia y que no vayan en detrimento de las libertades civiles. Durante el verano de 2016, después del atentado en Niza, la Secretaría Política del partido difundió un informe con medidas para combatir a Daesh, como, por ejemplo, cortar las vías de financiación y y abastecimiento logístico del grupo terrorista, neutralizar sus redes de captación y adoctrinamiento, apoyar a las fuerzas democráticas en el mundo árabe, acabar con la guerra en Siria e Irak, proteger a los refugiados, acabar con las mafias que trafican con personas y, por último "combatir la xenofobia que está tomando a los refugiados como cabeza de turco".

UNIDAS PODEMOS

CONCLUSIONES

Con todos los datos e informaciones obtenidas, los partidos entrevistados dan a entender, en general, que la legislación y la forma de luchar contra el terrorismo y la radicalización violenta es mejorable. Salvo el PSOE que afirma con contundencia que le parece correcto lo que está ejecutando el Gobierno en materia antiterrorista y antiradicalización, los demás consideran que es necesaria la introducción de nuevas y renovadas medidas para acabar con este fenómeno.

Aunque exista discrepancia entre los diferentes actores políticos, podíamos afirmar que todos tienen presente la necesidad de unión para luchar contra el terrorismo. Cada uno de ellos ha propuesto diferentes medidas que considera fundamentales; por ejemplo, el PSOE da importancia a la colaboración entre los diferentes organismos nacionales (Policía Nacional, Guardia Civil, CITCO); el PP, aunque explica que se deben mejorar ciertas áreas, como la prohibición de homenajes a etarras, da prioridad a la colaboración europea; Cs basa su estrategia en la prevención de la radicalización violenta a través de la educación y la creación de un Observatorio que estudie el fenómeno; y por último, desde VOX son más críticos con el Gobierno, dando prioridad al control de las fronteras y al freno de la inmigración ilegal.

Por último, desde su programa, Unidas Podemos sólo da unas pinceladas acerca de sus medidas contra el terrorismo, ciñéndose a lo estipulado por la Unión Europea y dando más importancia a las causas sociales indirectas del terrorismo más que a la lucha contra el fenómeno en sí.

Autor: Vera de Benito Ortega. Periodista y politóloga. Especializada en Seguridad Nacional y Terrorismo. Titulada en Criminología.

El Supremacismo Blanco en Estados Unidos: una Amenzaza Infravalorada

Resumen: Con los atentados a las Torres Gemelas el 11 de septiembre de 2001 se produjo un cambio de paradigma en la estrategia y la perspectiva contra el terrorismo por parte de las agencias de inteligencia, las fuerzas de seguridad y las fuerzas de la ley. Desde entonces, los esfuerzos se han centrado en su mayoría, a abordar la amenaza del yihadismo. No obstante, a raíz de los últimos acontecimientos, siendo ejemplar el asalto al Capitolio de los Estados Unidos (2021), ha quedado al descubierto el impacto de este desequilibrio y la insuficiente preparación para responder con eficacia ante atentados terrorista y acciones violentas por parte del extremismo violento doméstico.

EL LEGADO HISTÓRICO

La creencia en la supremacía blanca y el racismo son inseparables de la fundación de los Estados Unidos, pues a lo largo de la historia del país han gozado de permisibilidad y soporte político y legal. La esclavitud de personas negras fue una práctica, aunque intrínsecamente violenta, habitual, legal y legitimada en el siglo XIX. A su abolición legal, no sin una reacción impetuosa por parte de los movimientos antiabolicionistas, le siguieron las leyes de segregación racial de Jim Crow (1877 – 1964) y otras leyes discriminatorias que privaban de derechos y libertades, las cuales no afectaban únicamente a la comunidad negra, como fue la Chinese Exclusion Act. Este marco legal de discriminación racial se complementó con un proceso de criminalización y deshumanización hacia estos colectivos, pero en especial hacia la población negra. Con la posterior firma del Pacto Internacional de Derechos Civiles y Políticos y el fin de la segregación racial, el supremacismo blanco permaneció enraizado en varios sectores de la sociedad norteamericana y grupos de extrema derecha. No obstante, el peligro que suponía el supremacismo blanco quedó eclipsado, una vez más, por la entrada en acción del terrorismo yihadista, especialmente en década de los 90 con el atentado fallido en el World Trade Center (1993), el doble atentado en las embajadas norteamericanas de Nairobi y en Dar es Salaam (ambos en 1998) o el atentado contra el USS Cole (2000) en el puerto de Adén (Yemen). Y habidas cuentas del 11-S, la emergencia de la amenaza yihadista fue declarada de máxima prioridad, a pesar de que Estados Unidos sufría a la par una nueva oleada de atentados vinculados al supremacismo blanco como el asedio de Ruby Ridge (1992) o el atentado de Oklahoma City (1995). Como consecuencia, el interés por el terrorismo doméstico mermó significativamente. Ya en 2005 el Departamento de Seguridad Nacional disponía apenas de recursos destinados a la investigación y al análisis de amenazas terroristas no yihadistas, aunque se hacía evidente tanto la persistencia como el aumento del número de ataques y complots perpetrados por la extrema derecha y el supremacismo blanco en el interior del país. En lo sucesivo, la sociedad norteamericana ha sido testigo de cuantiosos ataques perpetrados por personas o grupos afines al supremacismo como el tiroteo en la Iglesia de Charleston (2015), el tiroteo de la Sinagoga de Pittsburgh (2018) y tiroteo de El Paso (2019). Eventualmente en 2019, ante tales evidencias, el Departamento de Seguridad Nacional de Estados Unidos anunció que el supremacismo blanco se posicionaba como la amenaza principal y más letal a la que se enfrenta el país.

EL SUPREMACISMO BLANCO EN UN ÁNGULO MUERTO

Hay un debate abierto sobre las razones de esta tardía reorientación de la atención y de los esfuerzos para contrarrestar las principales amenazas del país. Un par de años atrás, el Departamento de Justicia confesó que

las autoridades tanto estatales como locales han sido más bien negligentes en reportar delitos de odios y ataques protagonizados por supremacistas y nacionalistas blancos. Hay quienes han resaltado la infiltración de supremacistas blancos entre las fuerzas de seguridad y de la ley. Otros han remarcado la falta de ímpetu político, especialmente durante la presidencia de Donald Trump y la escasez de herramientas y de coordinación entre los diferentes niveles administrativos, agravado por la falta de una definición universal de terrorismo. Y aunque es cierto que la sección 802 de la USA PATRIOT ACT recoge una definición de terrorismo doméstico, esta ley junto al resto de leyes contra el terrorismo internacional adoptadas tras el 11-S, están focalizadas a afrontar unas circunstancias determinadas. Por eso, no pueden ser un modelo para responder a la violencia política interna, pues la violencia motivada por el supremacismo parte de una coyuntura histórica y política distinta. Además, pese a que las leyes antiterroristas de los estados establecen un delito sustantivo para el terrorismo doméstico, no existe una ley federal para esta tipología de terrorismo y por lo tanto, no hay un delito federal.

No obstante, es también evidente la distorsión de la categoría terrorismo, ya que hay una tendencia a evitar calificar como terrorismo la violencia cometida por el extremismo de derechas del país. Por lo general, el gobierno estadounidense preferentemente utiliza el término extremismo violento doméstico (DVE por sus siglas en inglés). En consecuencia el acento está en el concepto violencia, que recae en la categoría de delito común, como asalto, secuestro, o asesinato, para lo cual ya existen leyes penales. En este escenario laxo, hay otra dificultad añadida: los actores individuales (erróneamente conocidos como lobos solitarios), los grupos informales y la violencia descoordinada (*Leaderless resistance*), una práctica más difícil de atajar y que se ha vuelto cada vez más habitual, en parte debido a la hiperconectividad que ofrece internet.

La invisibilización del supremacismo blanco también es el resultado de la construcción de la imagen del terrorista casi exclusivamente como la de una persona extranjera y lejana, esencialmente árabe y/o musulmana. La propaganda y los medios de comunicación han reforzado esta errónea percepción a través de una conceptualización, en ocasiones estereotipada y sesgada y una cobertura mediática desproporcionada de sucesos específicos, como pone de manifiesto un estudio que señaló que los ataques terroristas de etiología yihadista habían recibido, en promedio, un 357% más de cobertura mediática que otros ataques. Si bien es cierto, que originalmente la extensa cobertura mediática respondía al impactante atentado, sin precedentes en el país, del 11-S, y a la posterior Guerra contra el Terrorismo.

En suma, como consecuencia de estas deficiencias, las políticas e iniciativas antiterroristas e incluso las medidas de prevención y detección del extremismo violento de derechas resultan ser ineficientes e insuficientes.

DONALD TRUMP: "MAKE AMERICA GREAT AGAIN"

La irrupción en el escenario político de Donald Trump es clave para comprender el clima de fanatismo actual en EUA. Ya desde el inicio de la campaña electoral de 2016, D. Trump se ha caracterizado por el uso de una retórica agresiva y dicotómica, cuyos objetivos eran (y son) colectivos étnicos y religiosos, los medios de comunicación, incluidos periodistas, y políticos, en su mayoría de la oposición. n discurso con el que se han identificado, en especial, personas afines y vinculadas al supremacismo y al nacionalismo blanco así como de grupos ideologías de extrema derecha, de ultraderecha, de la alt-right y la alt-lite.

La sociedad, en general, también se ha hecho eco de esta narrativa odiosa y estigmatizadora, que en voz del ahora expresidente queda legitimada e incluso normalizada, como puso de manifiesto Race in America 2019. El informe expuso que el 65% de los americanos consideran que en la actualidad es más común la manifestación de opiniones y posturas racistas. En especial, más de cuatros de cada diez personas norteamericanas, sostienen que estas expresiones se han vuelto más tolerables. Incluso varios informes y estudios han constatado una correlación entre D. Trump y el aumento de violencia y crímenes de odio contra minorías y colectivos. "La violencia lingüística ejercida por el poder es particularmente peligrosa" y es ilustrativo su discurso "Save America" , que alentó al asalto al Capitolio.

Durante su mandato, Donald Trump, cuyo jefe de estrategia y alto consejero fue el conocido supremacista Steve Banon, ha relativizado el potencial peligro del supremacismo blanco a pesar de las advertencias. Contrariamente a los datos y evidencias, Trump ha exagerado la amenaza de grupos y movimientos ideológicamente opuestos como el movimiento Black Lives Matter o ANTIFA, al que Trump quería calificar como organización terrorista.

Su falta de interés, también, quedó evidenciada por los recortes de los fondos para prevenir y combatir el terrorismo doméstico o su propósito para renovar el programa "Countering Violent Extremism" bajo el nombre de "Countering Islamic Extremism".En definitiva, cambios que reflejaron que contrarrestar el supremacismo blanco no entraba en su agenda. Asimismo, ha demostrado tener cierta proximidad con grupos supremacistas como los Proud Boys, a quienes en vez de condenar en su momento, los alentó a "retroceder y esperar" ("stand back and stand by", frase que ha pasado a ser parte del logotipo del grupo). De hecho, los supremacistas blancos aplaudieron la victoria electoral de D. Trump y verbalizaron en repetidas ocasiones, su satisfacción y alegría. Andrew Aglin, conocido neonazi y supremacista blanco editor de The Daily Stormer (sitio web), declaró la era de Trump, "la era de la venganza". En palabras de Mark Potok, experto en la derecha radical, "la candidatura de Trump electrificó a la derecha radical, que vio en él un defensor de la idea de que Estados Unidos es fundamentalmente un país de hombres blancos"

JOE BIDEN: ¿UN NUEVO ENFOQUE?

Tras el asalto al Capitolio de los Estados Unidos, afloró de nuevo el debate sobre cómo poner freno a la oleada de extremismo violento doméstico, en especial al supremacismo blanco. Sin embargo, el asunto es espinoso por razones políticas, legislativas y culturales y es quizá el mayor desafío legal —y políticamente, la empresa más delicada— que esta nación se ha enfrentado desde la Guerra Civil.

Aun así, poco después de tomar el cargo, Joe Biden ha dibujado un escenario más esperanzador para abordar el supremacismo blanco y hasta la fecha, ha demostrado un compromiso y una intención firme para socavarlo. Por un lado, tomando nuevas medidas e iniciativas para combatir el terrorismo doméstico y el supremacismo blanco, entre las que cabe destacar el hecho de que prometiera trabajar para la aprobación una nueva ley para afrontar el terrorismo doméstico e incrementar el presupuesto destinado a atender la emergencia del supremacismo blanco.

Además, a diferencia del expresidente D. Trump, J. Biden no ha titubeado en reconocer públicamente el supremacismo blanco como la mayor y más letal amenaza con la que tiene que lidiar en el país y ha calificado el asalto al Capitolio como terrorismo doméstico.

Por otro lado, también ha evidenciado su intención de las divisiones y tensiones raciales y la eliminación de la discriminación racial, una labor necesario para prevenir el odio, la discriminación y la violencia motivada por razones de raza, etnia y religión.

PRINCIPALES ORGANIZACIONES SUPREMACISTAS

Principales grupos y organizaciones supremacistas				
Grupos / organizaciones paramilitares	**Grupos Neo-nazis / Neo-fascistas**	**Grupos neo-confederados**	**Prision gangs**	**Christian Identity**
Proud Boys (Canadá)	**Atomwaffen Division** (Inglaterra, Canadá, Australia)	League of the South	Aryan Brotherhood of Texas	**Aryan Nations**
Oath Keepers	**Hammerskin Nation** (España)	Ku Klux Klan	Saxon Knights	Phineas Priesthood
Three Percenters	Nationalist Front (coalición)	East Coast Knights of the True Invisible Empire	Southern Brotherhood	Assembly of Christian Soldiers
The Base (Canadá)	Patriot Front	Loyal White Knights of the Ku Klux Klan	Aryan Circle	Church of Jesus Christ–Christian
Boogaloo Movement	Vanguard America	Council of Conservative Citizens	Unforgiven	Kingdom Identity Ministries

- Amenaza terrorista (EUA)
- Organización terrorista (denominados por otros países)
- Organización ilegal (denominados por otros países)

En la actualidad el supremacismo blanco es un fenómeno complejo que subyace en numerosos grupos, organizaciones y pandillas con ideologías extremistas similares, como ilustra la siguiente tabla. Su principal nexo común es la voluntad de salvaguardad la "pureza racial" y la superioridad de las personas blancas. En su mayoría son de naturaleza violenta y agresiva.

En varias ocasiones miembros vinculados a estas organizaciones han sido detenidos, juzgados o condenados por diferentes delitos y crímenes, con frecuencia motivados ideológicamente, como acoso, robos, actos vandálicos, agresiones, asesinatos, conspiración para cometer atentados o fabricación de explosivos. Y a pesar de que en el país coexisten centenares de organizaciones extremistas supremacistas cuyas características coincidirían con la de definición de organización terrorista, no existe una lista de grupos terroristas domésticos como si es el caso de las organizaciones terroristas extranjeras. El motivo de su ausencia subyace en la falta de una ley común e indivisa sobre el terrorismo interior.

Autora: Laura Illa. Especializada en seguridad y políticas de prevención de la extrema derecha y la extrema izquierda y colaboradora de Sec2Crime en la sección de Terrorismo y Conflictos Armados.

Las mujeres en los delitos sexuales

Resumen:Los delitos sexuales cometidos por mujeres representan un porcentaje muy pequeño, pero esto no resta importancia a la gravedad de los mismos. Debido a sus características existe una gran "cifra negra", ya que la mayoría son cometidos sobre menores. En este artículo se mostrarán algunas de las tipologías y perfiles de estas agresoras sexuales.

ALGUNOS DATOS

Este tipo de delitos son muy escasos en las mujeres. Concretamente, según los datos del INE de 2019, tan solo supusieron un 0,13% del total de delincuencia femenina. En cuanto a los hombres, estos fueron 1% del total de delincuencia masculina. En comparación, los delitos sexuales cometidos por hombres suponían el 97% aproximadamente, y por mujeres un 3%. Al haber tan pocos casos conocidos sobre estos delitos cometidos por mujeres, podemos entender que existe una ausencia de estudios sobre este hecho delictivo.

¿UNA MUJER TE PODRÍA VIOLAR?

Cuando hablamos de delitos contra la libertad e indemnidad sexual es muy importante diferenciar entre el abuso sexual y la agresión sexual.Popularmente, existe la creencia de que la discrepancia entre estos tipos penales es la penetración, pero es falso. Su diferencia radica en la presencia o no de "violencia e intimidación" y en el "consentimiento". Así pues, en el Código Penal encontramos:

Artículo 178 C.P. "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."

Artículo 181 C.P. "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 dieciocho a veinticuatro meses."

Por otra parte, tendríamos la violación, en la que sí es necesaria la presencia de penetración. Este tipo delictivo es el que puede tener una mayor controversia en cuanto a que pueda ser cometido por una mujer, pero tenemos que tener en cuenta que la penetración no tiene por qué ser mediante el miembro viril por la vía vaginal. Del mismo modo, el Código Penal expone:

Artículo 179 C.P. "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."

Por ello, pese a que de primeras nos parezca extraño considerar que una mujer pueda cometer delitos contra la libertad y la indemnidad sexual, tenemos que ser conscientes de que pueden hacerlo y, además, en cualquiera de sus modalidades.

LA CIFRA NEGRA

En todos los delitos es muy importante tener en cuenta la "cifra negra"; el número de delitos y delincuentes que no son conocidos por la justicia. Sin embargo, en esta tipología la cifra podría ser mayor que en cualquier otra, incluso superior que en aquellos en los que el agresor es el hombre.

La falta de denuncia en estos casos, al igual que en la mayoría, son debido a que: las víctimas consideran los hechos poco relevantes, valoran que es inútil denunciar, desconfían del sistema de justicia o no quieren reconocerse como víctimas. Este último punto cobra más importancia en este tipo de delitos, en los que de por sí se estigmatiza al denunciante, y más aún si la denuncia proviene de un hombre contra una mujer, debido a los roles de género y a su relación con la sexualidad. Por lo tanto, esto va a generar una victimización secundaria en el sujeto por la que no quiere pasar.

Además, la mayoría de estos delitos se cometen contra menores o adolescentes. Aquí, nuevamente, un factor muy importante es el rol de géneroasociado a la maternidad de la mujer. Esto hace que en muchas ocasiones esa cercanía que pueden tener con los menores no llame tanto la atención e incluso, que cuando se trate de adolescentes estos no sean conscientes de lo que está sucediendo, llegando a considerarlo fantasías incestuosas. Además, cuando la agresora es su propia madre esto se vuelve mucho más complicado.

PERFIL DE LA AGRESORA SEXUAL

Podríamos establecer un perfil general sobre mujer agresora sexual con las siguientes características:

- La edad suele comprender entre los 22 y 33 años.
- Un gran porcentaje de ellas había sufrido abusos sexuales y violencia física, incluso en el ámbito intrafamiliar.
- Muchas tienen antecedentes de abuso de alcohol y drogas.
- Existe prevalencia de problemas depresivos, paranoicos y de personalidad límite o dependiente.
- Tienen baja capacidad de afrontamiento, sentimientos de inferioridad e inseguridad.
- Su infancia y adolescencia ha estado marcada por la necesidad de satisfacer los deseos de los demás.
- Pueden pertenecer a distintos grupos sociales y tener diferentes niveles educativos.
- Tienen una vida sexual y marital inconstante y cambiante.
- Sus víctimas son desproporcionadamente jóvenes, menores de 18 años, y no se encuentran preferencias en cuanto al sexo.
- Al igual que la mayoría de los autores de este tipo de delitos, no reconocen los hechos ni se consideran responsables.

ALGUNAS TIPOLOGÍAS

Mathews, Matthews & Speltz (1991) elaboran una tipología que consta de 3 perfiles:

- **"Teacher-lover" (profesora amante):** no considera que esté llevando a cabo ningún tipo de delito. Ella cree que realmente tiene una relación con el adolescente "de igual a igual", por lo que piensa que se encuentra en una relación sentimental consentida. Pueden haber sufrido abusos sexuales en la infancia.

- **"The intergenerationally predisposed offender" (abusadoras predispuestas):** este tipo de agresoras actúan en solitario. Suelen abusar y agredir a niños conocidos o miembros de su familia, incluso a sus propios hijos. Han sufrido una victimización constante por abusos sexuales de diferentes tipos por varios miembros de su familia.
- **"The male coercer-offender" (abusadora forzada)**: en este caso la mujer actuaría por presión de un hombre, habitualmente su marido. Son dependientes de este y suelen ser abusadas por él también. Las víctimas normalmente son sus propios hijos.

Vandiver & Kercher (2004), dividen la **tipología en 6:**

- **Educadora heterosexual:** la edad media de estas mujeres es de 30 años, y abusan de niños de unos 12 años. Sería similar a la tipología de profesora amante de Mathews et al. (1989). Perciben la situación como una relación real y están motivadas por un deseo de intimidad para compensar las necesidades emocionales y sociales insatisfechas.
- **Agresora homosexual no delincuente:** mujeres con una media de edad de 32 años. Sus víctimas son niñas, con una media de 13 años. Es posible que puedan actuar con un cómplice masculino.
- **Depredadora sexual: t**ienen una media 29 años y sus víctimas eran niños de unos 11 años. En ellas el delito sexual es solo una parte de su carrera criminal.
- **Joven adulta explotadora de niños:** son las más jóvenes, con una media de edad de 28 años. Las víctimas tenían una media de 7 años, siendo tanto niños como niñas. Incluye víctimas conocidas y desconocidas y es probable que realicen agresiones sexuales.
- **Delincuentes homosexuales:** la mayoría de las víctimas eran niñas, con una media de 11 años. Las agresoras tienen una media de 32 años y realizan con ellos actos sexuales e incluso la prostitución. Su motivación es económica. Tienen una alta probabilidad de recaer en cualquier tipo de delito.
- **Delincuentes homosexuales agresivas:** Muy similares al tipo anterior, pero sus víctimas tienen una media de 31 años.

Wijkman, Bijleveld & Hendriks (2010) distinguen **4 perfiles:**La edad suele comprender entre los 22 y 33 años.

- **Jóvenes agresoras:** son mujeres jóvenes e independientes que abusan de niños que son familia o de los que están al cuidado. Se asemeja al tipo de joven adulta explotadora de niños de Vandiver & Kercher (2004).
- **Violadora:** generalmente sus víctimas son mayores y no tiene preferencias entre hombres o mujeres. Estas han sido abusadas sexualmente en su infancia por alguien externo a su familia. Sería similar a la depredadora sexual de Vandiver y Kercher (2004) y a la abusadora predispuesta de Mathews et al.(1991).
- **Coautoras con problemas psicológicos:** se caracterizan por la presencia de trastornos mentales. Tienen entre 30 y 35 años y actúan junto con una o más personas y ejercen delitos sexuales diversos. Las víctimas habitualmente son de la familia o conocidas, sin tener preferencia entre niños o niñas. Podría estar dentro de la tipología de abusadoras predispuestas de Mathews et al. (1991).

- **Madres pasivas:** tienen una edad media de 41 años, siendo las más mayores. No tienen un papel activo, ya que solo observan el abuso o facilitan que este se produzca. Normalmente es sobre sus propios hijos e hijas, con edades entre los 7 y 11 años. Sería similar al tipo de abusadora forzada de Mathews et al. (1991).

CONCLUSIONES

Se puede concluir que, generalmente, las mujeres que cometen delitos sexuales rondan los 30 años y suelen actuar sobre víctimas menores de edad, normalmente entre los 7 y 11 años. En muchas ocasiones actúan sobre miembros de su familia, incluidos sus hijos. Es importante destacar que esto tiene una gran influencia en la "cifra negra", debido a que en estos casos es más complicado que estos actos salgan a la luz, ya sea porque alguien lo descubra o, mucho menos, porque sean denunciados por el propio menor. Por lo tanto, los delitos sexuales cometidos por mujeres presentan un porcentaje muy pequeño, pero posiblemente la realidad sea distinta.

Autora: Ángela Martín García. Psicóloga especializada en análisis de la conducta criminal. Colaboradora del área de Criminología de Sec2Crime.

Misión en "Cumbre Vieja"

Resumen: La erupción del volcán "Cumbre Vieja", en la isla de La Palma, ha ocupado la mayor parte de las portadas de los telediarios desde el pasado 19 de septiembre. La lava ha cubierto más de un millar de hectáreas y más de 2.000 viviendas han sido arrasadas.

Al igual que en otras catástrofes naturales, como la borrasca "Filomena", que afectó principalmente al centro de la península a comienzos de 2021, las Fuerzas Armadas han contribuido en las labores necesarias.

La actuación se coordina dentro del Plan Especial de Protección Civil y Atención de Emergencias por Riesgo Volcánico en la Comunidad Autónoma de Canarias. A pesar de que la Unidad Militar de Emergencias es la que tiene un mayor número de efectivos desplegados, el Ejército de Tierra, el Ejército del Aire y la Armada han aunado esfuerzos para paliar los efectos de la erupción y prestar su ayuda al personal civil afectado.

VOLCÁN EN ERUPCIÓN

Varios seísmos se sucedieron los días previos a la erupción del volcán "Cumbre Vieja", localizado en la isla de La Palma. Este hecho sirvió para alertar de una situación que se prolongaría en el tiempo y acabaría dejando a muchas familias sin una parte importante de sus vidas.

El 19 de septiembre, pasadas las tres de la tarde, hora local, comienzan a emerger al exterior grandes columnas de humo y ceniza, a la vez que la lava se desprende en la zona de Cabeza de Vaca, en la localidad de El Paso.

Inicialmente, la Guardia Civil realizó la evacuación de, aproximadamente, 5.000 personas (Europa Press, 2021) y muy pronto la emergencia se extendió hasta el nivel rojo.

Fue solo el comienzo de una actuación en la que ha sido necesaria la colaboración de diferentes actores, entre los que se encuentran las Fuerzas Armadas (Fernández, 2021)

ANTECEDENTES

La Comunidad Autónoma de Canarias registra una importante actividad volcánica, algo que no ocurre en otros territorios de España. Sin embargo, no todas las islas del archipiélago han mantenido el mismo nivel de actividad durante los últimos años. Las de mayor intensidad son La Palma, Tenerife y El Hierro.

Lanzarote, considerada volcánicamente activa, ha tenido dos erupciones importantes, en 1730 y 1824. Gran Canaria, por su parte, no ha registrado actividad reciente, aunque sí durante los últimos 10.000 años. (Involcan, 2018)

En el caso de La Gomera y Fuerteventura el riesgo de que se produzca una erupción es relativamente bajo.

Solo durante el mes de septiembre, se sucedieron 1.600 terremotos en el área de las Islas Canarias. (Instituto Geográfico Nacional, 2021)

Erupción del volcán / José Ángel Cortés

EL PLAN ESPECIAL DEL GOBIERNO CANARIO

El Gobierno de Canarias dispone del Plan Especial de Protección Civil y Atención de Emergencias por Riesgo Volcánico en la Comunidad Autónoma de Canarias (PEVOLCA), aprobado por el Decreto 112/2018, de 30 de julio (Involcan, 2018). El objetivo es lograr una respuesta coordinada, ágil, eficaz y eficiente entre todas las administraciones públicas para hacer frente a crisis sismovolcánicas y a las emergencias derivadas de ellas.

El Plan surge tras los precedentes de Tenerife, en 2004, y en El Hierro, en 2011 y 2013. Durante la reciente erupción en La Palma el PEVOLCA ha servido para coordinar la actuación y unificar los procedimientos entre todos los involucrados.

LA ACTUACIÓN DE LA UME

Desde el mismo día en que se produce la erupción del volcán, la Unidad Militar de Emergencias (UME) movilizó efectivos en la zona. Los primeros en desplegar fueron algunos de los integrantes de la Unidad de Intervención en Emergencias de Canarias.

Posteriormente, se añadieron los 62 primeros efectivos que salieron desde la Base de "Los Rodeos", en Tenerife, en barco hasta La Palma. Un segundo equipo, con 64 militares de la UME, se sumó a ellos desde la Isla de Gran Canaria. Paralelamente, desde la península un avión A 400 del Ejercito del Aire desplazó otros 58 militares pertenecientes al II Batallón de Intervención de Emergencias (BIEM). Entre ellos iba un equipo de control de atmósferas del Grupo de Intervención en Emergencias Tecnologías y Medioambientales (GIETMA), procedente de Madrid. (Ministerio de Defensa, 2021)

Los efectivos de la Unidad Militar de Emergencias están integrados en el dispositivo que dirige el Gobierno de Canarias, siguiendo lo marcado en el PEVOLCA. De este modo, los militares del II Batallón han realizado labores de vigilancia y control para minimizar los daños colaterales provocados por el avance de las coladas de lava. También han acompañado y ayudado a los vecinos evacuados a recoger sus pertenencias personales.

Por su parte, el GIETMA se ha encargado de las labores de medición del aire, para prevenir posibles gases tóxicos, en colaboración con el personal de la Comunidad Autónoma de Canarias y del Instituto Geológico Nacional.

Para ayudar en estos cometidos se ha empleado un vehículo equipado con diferentes sensores para detectar, identificar y tomar muestras ambientales de posibles agentes químicos. Entre los más reconocidos en este tipo de situaciones se encuentran el monóxido de carbono, dióxido de azufre o el ácido clorhídrico, que se podría formar al entrar en contacto la lava con la sal del mar.

Para garantizar el apoyo, la UME ha establecido relevos de sus unidades y el Gobierno de Canarias ha demandado que se mantenga, por el momento, su presencia en la zona.

LA ACTUACIÓN DEL EJÉRCITO DE TIERRA

Una de las principales actuaciones que ha realizado el Ejército de Tierra ha sido la de proporcionar la logística necesaria para el alojamiento, seguridad o servicios del personal civil evacuado.

Tras la primera erupción, y en pocas horas, se pusieron a disposición de las autoridades civiles un millar de plazas de alojamiento. Las principales instalaciones que se han estado utilizando son las de la Unidad de Apoyo a la Protección (UAPRO) "El Fuerte", a las que se ha sumado el apoyo de personal y material de campamento de la Brigada "Canarias" XVI, encuadrada en el Mando de Canarias, y de la Quinta Subinspección General del Ejército.

Además, se ha alojado en "El Fuerte" a personal dependiente y con necesidades sanitarias especiales, merced al apoyo prestado por Cruz Roja y el Servicio Canario de Salud.

El Ejército también colabora desde estas instalaciones con la UME y otros implicados, apoyando con la infraestructura logística necesaria, en cuanto a alojamiento o seguridad, entre otros cometidos.

En definitiva, el Acuartelamiento ha servido como embrión para la proyección y despliegue inmediato de capacidades militares ante la emergencia. Disponer de esta UAPRO en las islas no capitalinas del Archipiélago se han probado como una capacidad estratégica para la ejecución ágil y eficaz de operaciones militares y de apoyo a autoridades civiles ante emergencias.
El día 13 de octubre se incorporó una sección del Regimiento de Artillería de Campaña 93 para colaborar en las labores de retirada de ceniza dentro de la zona de exclusión. Después les relevó otra sección del Regimiento de Infantería "Tenerife" nº 49 y el objetivo es ir realizando rotaciones semanales. También se han incorporado medios del Regimiento NBQ "Valencia" nº 1, para colaborar en las tareas de medición de calidad del aire. (Pulido, 2021)

APOYO A LOS AGRICULTORES

La Armada también se ha involucrado en la ayuda a los damnificados como consecuencia de la erupción del volcán "Cumbre Vieja". Desde el 11 de noviembre, las lanchas de desembarco del Buque de Asalto Anfibio "Castilla" están trasladando a los agricultores hasta aquellos terrenos que son de complicado acceso y que han quedado aislados como consecuencia de las coladas de lava.
El objetivo es que puedan atender y regar sus cultivos. El trayecto se realiza en, aproximadamente, 20 minutos y va desde el puerto de Tazacorte hasta la playa de Puerto Naos.
El Cabildo de La Palma solicitó la ayuda el 1 noviembre y tan solo una semana más tarde el Buque partía desde la Base Naval de Rota (Cádiz).
El "Castilla" llegaba integrado por 250 tripulantes y portaba cuatro lanchas, capaces de transportar a 80 personas cada una. No obstante, una treintena se han hecho cargo de las barcas y los desplazamientos. (EFE, 2021)

La intención es que la ayuda se mantenga el tiempo que sea necesario en la zona. Además, se irá adaptando a las necesidades de los agricultores.
Gracias a este apoyo se puede realizar este trayecto en un tiempo menor y contribuir así a salvar las cosechas que no han sido arrasadas por la lava.

CONCLUSIONES

- Las Fuerzas Armadas han prestado su apoyo ante la emergencia provocada por el volcán "Cumbre Vieja", desde el momento en que se origina la erupción, el 19 de septiembre.

- El dispositivo se ha integrado en el Plan Especial de Protección Civil y Atención de Emergencias por Riesgo Volcánico en la Comunidad Autónoma de Canarias.

- La actuación se ha desarrollado de manera rápida y coordinada. De hecho, un pelotón de Zapadores de la Brigada "Canarias" XVI, del Ejército de Tierra, que se encontraba realizando actividades de preparación se incorporó de inmediato al operativo.

- La Unidad Militar de Emergencias ha empleado el mayor número de personal, aunque ha sido fundamental el apoyo prestado por el Ejército de Tierra, el Ejército del Aire y la Armada.

- Las Fuerzas Armadas han participado, anteriormente, en otras catástrofes naturales, como la borrasca Filomena, a comienzo de 2021, por lo que una vez más demuestran el compromiso con la sociedad en momentos de extraordinaria necesidad.

-El volcán "Cumbre Vieja" mantiene su actividad sísmica (Instituto Geográfico Nacional, 2021) y de erupción, por lo que la actuación de las Fuerzas Armadas,por el momento, se mantendrá, tal y como ha solicitado el gobierno de las islas.

BIBLIOGRAFÍA

- EFE. (10 de Noviembre de 2021). Obtenido de https://www.efe.com/efe/canarias/sociedad/la-armada-facilitara-a-los-agricultores-de-palma-el-acceso-sus-fincas/50001312-4672663

- Europa Press. (19 de Septiembre de 2021). Obtenido de https://www.europapress.es/islas-canarias/noticia-marcha-evacuacion-mas-5000-personas-erupcion-cumbre-vieja-palma-20210919203916.html

- Instituto Geográfico Nacional. (12 de Noviembre de 2021). Obtenido de https://www.ign.es/web/resources/volcanologia/html/CA_noticias.html#20211112

- Instituto Geográfico Nacional. (Noviembre de 2021). Obtenido de https://www.ign.es/web/resources/volcanologia/html/CA_noticias.html#202109

- Involcan. (2018). Obtenido de https://www.involcan.org/wp-content/uploads/2018/10/boc-a-2018-154-3785.pdf

- Ministerio de Defensa. (21 de Septiembre de 2021). Obtenido de https://www.defensa.gob.es/ume/noticias/2021/09/Noticias/volcan-la-palma.html

- Pulido, F. (Noviembre de 2021). Volcán en erupción. Tierra, pág. 4.

Autor: Felipe Pulido Esteban. Periodista. Colaborador del área de Defensa Nacional Sec2crime.

Informática Forense: Integración en la investigación policial

Los sistemas informáticos actualmente son considerados como la central de almacenamiento de datos con enorme valor, siendo vulnerables debido al desplazamiento por el ciberespacio.

La llamada ciberdelincuencia inicia desde una búsqueda de información ilegal hasta acceder, interferir, abusar, falsificar datos y sistemas, los cuales ya están tipificados en el Código Penal y convenios como es el Convenio Budapest 20011.

Aquella forma de delinquir se ha ubicado en todas las esferas digitales, intensificando su desarrollo y creación de nuevo delitos. Las escenas delictivas, autores, instrumentos y sobre todo modus operandi se transforman de la mano de la era digital y es así como la ciberdelincuencia se posiciona con fuerza en la red informática mundial.

Los dispositivos a través de los que se ejecutan los ciberdelitos guardan indicios en el plano digital y físico, por lo que es indispensable el conocimiento pleno en Informática Forense, ciencia capaz de examinar una escena digital e identificar los demás elementos del ciberdelito y así obtener investigaciones con gran valor policial y judicial.

La red contiene vacíos de seguridad y la ausencia de un uso responsable de las mismas por parte de la población, lo que la convierte en vulnerable, así pues, la virtud identificativa y analítica de la informática forense genera una esperanza de seguridad en el entorno más transitado, el internet.

Las actividades cotidianas giran en torno al uso de la red de modo que información personal recorre esferas digitales peligrosas, las que luego se utilizan para ejecutar un sin número de ataques como por ejemplo fraude, acoso y extorsión.

INCIDENTES EN LA CIBERSEGURIDAD

Los sistemas informáticos pueden verse atacados en su estructura de modo que en el momento de la ejecución la seguridad se verá afectada y disminuirá su eficacia. Los incidentes tienen un ciclo de vida de modo que se puede aplicar un proceso para su investigación.

El descubrir es la primera fase de cualquier ataque ya que el ciberdelicuente, investiga la seguridad de los activos, horarios, información pública para ejecutar el ataque, seguidamente profundiza en el tipo de sistema al que se va a enfrentar.

De modo que conocer más sobre la dirección de red, nombres de dispositivos, servidores y más datos, todo ello va a conocer mediante la aplicación de instrumentos detectores, scanner y programas que permitan analizar las conexiones y configuraciones establecidas.

Hasta este punto todas las técnicas que se utilizan por parte del ciberdelicuente no permitirán su detección, de modo que el ataque planeado se detonará el día de su ejecución. Seguidamente inicia un proceso de vulneración del sistema y finalmente interceptan y obtienen el control del sistema.

INFORMATICA FORENSE

La informática forense surgió como necesidad para tratar delitos en los que mediaba evidencias digitales, identificación y recolección de estas con el objetivo de interpretar y presentar indicios que tengan valor de prueba, adquiriendo capacidad para investigar esta tipología de delitos.

Las ciencias forenses tienen el objetivo de utilizar recursos científicos para investigar hechos delictivos físicos y también delitos cibernéticos y para ello es necesario un análisis forense de equipos electrónicos, datos informáticos, sistemas y más con la finalidad de lograr, interpretar y responder a la Administración de Justicia.

La informática forense establece sus principios básicos de actuación para que de ellos se desprenden como resultado eficacia y credibilidad y son:

- Organización y documentación detallada
Este principio descansa en la labor del investigador, el desarrollo de una investigación documentada y enumerada va a permitir comprender las conclusiones y comparar con otros análisis de manera objetiva.

De tal forma la investigación se va a caracterizar por ser veraz, integra y eficaz guardando la profesionalidad del investigador y sin temor alguno se puede practicar nuevas investigaciones al mismo indicio y se obtendrán resultados similares.

- Integridad de la evidencia
Uno de los principios más importantes dentro de la informática forense es garantizar la integridad de la evidencia de modo que se asegura la negativa de alterar el proceso de la investigación y los elementos de este, de modo que la llamada cadena de custodia debe cumplir con la eficacia en la preservación de las evidencias y para ello es necesario aplicar las medidas y practicas correctas.

- Validación de la cadena de custodia
El procedimiento de la cadena de custodia se rige bajo estatutos y normas establecidas, como son las diligencias de información e informe, del cual se obtiene como fundamento para corroborar cada uno de los pasos de este proceso.

ESCENA DEL DELITO

El escenario en el que se ejecuto el hecho delictivo es la fuente de información junto con los indicios para la investigación, es por ello por lo que el tratamiento debe ser cauteloso. De modo que se hace imprescindible abordar el escenario para comprender paralelamente el escenario digital y la labor de los investigadores en el mismo.

La observación consiste en una de las primeras diligencias al llegar al lugar y de forma inmediata apuntar el estado y características del área, idénticamente en el caso de los delitos informáticos se procede a observar si el delito continúa perpetrándose a través de dispositivos a los sistemas informáticos o están en condición de víctimas. Esta diligencia acapara todas las redes, sistemas y dispositivos que se encuentren en la escena.

RECONSTRUCCIÓN DE LA ESCENA CIBERDELICTIVA

El objetivo de la reconstrucción es interpretar la relación evidencia, víctima y escena del crimen, de modo que da luz al investigador para comprender el modus operandi y desarrollo del ciberdelito, mediante aquello se recurre a la reconstrucción.

Una evidencia física es cualquier elemento que este relacionado con el autor y la escena, considerando elementos como medios o herramientas para ejecutar el hecho delictivo, elementos que han sido despojados. La evidencia digital puede tener su ubicación en varios continentes, simplemente con un clic en segundos se puede transferir un sin numero de información a su vez se puede emitir copias sin afectar su calidad y sobre todo tiene un ciclo de vida, el tiempo y el cumplimiento de su objetivo darán fin a cada una de las evidencias.

INVESTIGACIÓN FORENSE

Solicitud Forense: Este primer paso se va a llevar a cabo cuando se esté ante un incidente y se alerte del mismo para solucionarlo, ya que en este caso el apoyo de la primera recolección de información general es llevada a cabo por los equipos responsables.

Adquisición: Como bien dice es la adquisición o recopilación de la primera información que circula en la escena, sea por los principales organismos que llegaron, testigos o denuncias, seguidamente la fijación fotográfica es esencial para evitar alteraciones en la cadena de custodia.

Todos los elementos que se encuentren en el lugar deben ser posibles indicios de modo que no hay perder la importancia de la recogida. En base a ello el investigador planifica una serie de preguntas orientativas y permite la construcción de la investigación.

Ubicar el espacio a investigar : Una vez que se cuente con la información general de los hechos, hay que verificar ante el caso que se está y determinar si el examen forense se lleva a cabo in situ o en el laboratorio.

La investigación tiene dos escenas para ser analizadas y estudiadas, la primera es la investigación física o in situ o escena en caliente y la investigación en el laboratorio, son las escenas distintas por las características de los indicios o evidencias.

Son dos escenas de gran responsabilidad ya que todas las evidencias independientemente cual sea su ubicación o trascendencia son testigos fieles de aquel delito y hay que identificar de forma segura. De modo que todos los indicios identificados en cada escena deben ser objeto de estudio evitando contaminarlos en lo posible.

Preservación y Transporte : Todos los datos obtenidos deben ser guardados y preservados como evidencias de modo que se elaboran fichas para describir lo que se ha encontrado, etiquetarlas, empaquetarlas y enviarlas al laboratorio.

Documentar: En el tratamiento de evidencias documentar es detallar las características de cada evidencia para constar, sin embargo, en este apartado la documentación es más administrativa, de modo que se va a determinar la ubicación de la evidencia, personal autorizado a utilizarla y tiempo de permanencia en el lugar.

Se debe localizar la evidencia, especificar sus características incluyendo soporte en el que se encontraba, tipo, marca, modelo, color y ubicación en relación con el dispositivo central y dispositivo inalámbricos, finalmente cumplimentar los formularios de custodia.

Las fotografías son un medio de investigación práctico, pero para reconstruir la escena sin problema, hay que hacer uso de plantillas y etiquetas para diferencias los indicios y tamaños en el material fotográfico.

HERRAMIENTAS DE ANALISIS FORENSE

Herramientas Forenses ToolKit: Son aplicables únicamente a sistemas Windows, estás presentan la capacidad de recoger datos e información y sobre todo programas o aplicaciones que van a permitir obtener informes y grupos de archivos para poder analizar.

The Sleuth Kit y Autopsy. :Una de sus funciones principales es analizar eventos de forma individual y múltiples, así también consta con acceso a archivos eliminados, agenda de contactos, imágenes y actividades del sistema, incluso dentro de estas herramientas se puede crear notas y desarrollar informes.

Herramientas editoras :GHEX y WinHEX son útiles para editar archivos, dispositivos, memoria de almacenamiento y sobre todo cumplen la función de recuperador de archivos eliminados.

Herramientas para recuperar contraseñas. : NtpwediT, funciona como software para modificar, recuperar y eliminar contraseñas solo en ciertas versiones de Windows como 7 y 8. Así también Jonh The Ripeer, Ntpasswd.

CONCLUSIONES

La informática forense se ha convertido en una disciplina indispensable para el desarrollo de investigaciones en relación con ciberdelitos, con anterioridad a su aplicación se usaban herramientas y estrategias de análisis informáticos generales obteniendo resultados mínimos.

El objetivo principal de esta disciplina es lograr identificar todos los elementos que constituyen un hecho ciberdelictivo análogamente como se llevan a cabo en delitos tradicionales.

A través de la profundidad de la investigación se localizarán nuevas formas ciberdelictivas y va a ser posible paliar y detener su ejecución. En cuanto a la práctica de análisis forense se conocerán las nuevas estrategias y elementos utilizados por los grandes ciberdelincuentes.

KAROL HERNÁNDEZ
CRIMINÓLOGA, MÁSTER EN INVESTIGACIÓN POLICIAL

Todo sobre las Filtraciones de Datos

Hace unos días tuvimos noticia de que una de las mayores filtraciones de datos de la historia podía descargarse en línea. Con más de 3.200 millones de registros, se considera la madre de las filtraciones. Pero ¿Qué es una filtración? ¿Cómo se produce y como nos afecta? Sigue leyendo para saberlo todo.

LA NUEVA SE LLAMA <COMB>

Esta semana se publicaron diversas noticias hablando sobre las filtraciones de datos, especialmente la llamada "COMB". Una recopilación en una extensa base de datos donde se reúnen toda la información procedente de las diferentes filtraciones de datos.

Este término alude a la recopilación de los datos expuestos que se han producido a lo largo de historia de internet. En los últimos años se ha constatado que incluso los servicios más grandes y más utilizados han sufrido este tipo de exposición de datos (LinkedIn, Adobe e incluso Facebook).

Por lo tanto, podemos entender como filtraciones de datos cuando usuarios internos o externos que utilizan artificios tecnológicos obtienen un privilegio de acceso a la información. A través de este obtienen datos personales de sus empleados o clientes. A menudo estos datos son personales, comprendiendo algunos como correos electrónicos y contraseñas, números de teléfono e incluso documentos de identidad.

UN POCO DE CONTEXTO SOBRE LAS FILTRACIONES DE DATOS

Para dar un poco de contexto, hay que entender que cada año este tipo de ciberataques aumenta. La seguridad de los servicios sigue siendo uno de los eslabones que necesitan de una mayor revisión por su actual debilidad.

La seguridad es algo que debe actualizarse de forma continua ya que los ciberdelincuentes siempre llevan un paso de ventaja.

Desgraciadamente no tiene la atención que debería ser necesaria, aunque los organismos internacionales están trabajando en ello.

Solamente en 2020 se han producido varios ataques que tienen como resultado la exposición de datos de miles de usuarios. Sucedió en mayo de 2020 con la compañía EasyJet, que reportó una brecha de seguridad en la que fueron expuestos más de 9 millones de clientes. También la filtración de Nintendo, que comunicó que habían comprometido alrededor de 300.000 cuentas de usuarios.

PERO ¿CÓMO SE PRODUCEN ESTAS FILTRACIONES DE DATOS?

Como comentábamos anteriormente, la seguridad es un proceso que debe ir creciendo. Esto debe hacerse con una mejora y con una actualización diaria por parte de los responsables de la misma. Las vulnerabilidades existen, no se ha inventado (todavía) un sistema que sea 100% seguro, y esto los ciberatacantes lo saben.

Además de las brechas de seguridad, también se dan muchos casos en los que el motor del ataque ha sido la ingeniería social. A través de este tipo de interactuaciones se pueden conseguir previamente credenciales que permitan el acceso a los datos críticos.

Un ejemplo común son los fallos humanos, donde un posible error puede exponer los datos que son considerados críticos. Un ejemplo de esto podríamos observarlo en las campañas de phishing, donde solamente con que uno de los empleados que lo reciben fueras ingenuo y accediera a los enlaces maliciosos ya causaría un daño considerable.

O también por medio de lo que se conoce como "Insider Threat". Es decir, una amenaza contra la seguridad o los datos de una organización que proviene de alguien cercano o conocedor de la compañía, como pueden ser empleados, exempleados, proveedores o clientes.

¿Y POR QUÉ SE PRODUCEN?

Muy sencillo. Tus datos valen dinero. Probablemente, mucho dinero. Las filtraciones de datos son muy rentables. Las empresas guardan muchos datos de sus clientes, nosotros mismos los otorgamos cuando nos registramos en alguna página web.

La obtención de estos datos por parte de cibercriminales puede derivarse en una venta de los mismos, ya que existen mercados donde el producto principal son tus datos y se comercia con estos por importantes sumas de dinero. No es el primer escándalo que surge a raíz de esta venta de datos.

También puede derivarse en más ciberataques, como podrían ser las campañas de phishing dirigidas (o llamadas "spear-phishing") con el objetivo de sacarle el dinero a la gente mediante engaños u otros más sofisticados como la famosa estafa del CEO.

¿CÓMO PUEDO SABER SI HE SIDO VÍCTIMA DE UNA DE ESTAS FILTRACIONES?

Existen diversas herramientas en línea que permiten comprobar si una cuenta de correo electrónico ha sido filtrada, como podrían ser los recursos de haveibeenpwned o la herramienta de Cybereop.

En estas herramientas que almacenan las diferentes filtraciones de datos, basta con introducir tu correo electrónico y el buscador realizará una comparativa para saber si lo que tu has introducido se encuentra expuesto.

También puedes mantenerte al día de las noticias sobre los ciberataques que se producen y si estás utilizando uno de los servicios que han sido atacados, probablemente tus datos puedan ir incluidos en el paquete.

VALE, YA HE COMPROBADO QUE MIS DATOS SE ENCUENTRAN EXPUESTOS, ¿ Y AHORA QUE HAGO?

Muy sencillo, tal y como recomendábamos en nuestro artículo anterior "¿Es tu contraseña segura?" uno de los primeros pasos a seguir es cambiar las contraseñas que se encuentren relacionadas con los fatos filtrados.

Recuerda que si utilizas la misma contraseña para varios servicios, deberás cambiar la de todos ellos. Además puedes basarte en nuestras recomendaciones para crear contraseñas seguras.

También, en todos los servicios que sea posible, es recomendable habilitar el doble factor de autenticación, ya que esto nos otorga una capa de protección adicional y que hará un poco más difícil los accesos a nuestras cuentas de correo o redes sociales.

CONCLUSIONES

A pesar de que la ciberseguridad es un campo que actualmente se encuentra en auge y cada vez tenemos un mayor conocimiento de los riesgos que implica el uso de internet, los ciberdelincuentes van un paso por delante y se mantienen constantemente actualizados.

Valiéndose de la premisa de que no somos capaces de crear un sistema perfecto que no contenga fallo de seguridad alguno, hace que nuestros datos sean vulnerables y por lo tanto, siempre estemos expuestos. El gran ejemplo son las filtraciones de datos, como hemos mencionado. Sin embargo, podemos ser optimistas, a través de las nuevas leyes que están surgiendo y de la toma de conciencia que se está realizando tanto en la población general como en empresas y servicios, cada día estamos un poco más "ciberseguros".

AINOA GUILLÉN
CRIMINÓLOGA, ANALISTA DE CIBERINTELIGENCIA

Criptografía: historia y curiosidades, la importancia hoy en día

La criptografía se ha utilizado desde hace miles de años, y actualmente está cada vez más presente en nuestro día a día, aunque la mayoría de las veces no nos damos cuenta.

Mantener mensajes en secreto nunca ha sido una tarea fácil pero el ser humano siempre ha intentado elaborar nuevos métodos para conseguirlo. La criptografía se ha usado desde tiempos inmemorables para transmitir información de unos a otros sin que los posibles interceptores tuviesen acceso a ella. En este artículo hablaremos sobre la historia de la criptografía, algunos de sus términos más básicos para poder entender cómo funciona y la importancia que tiene hoy en día en las actividades más cotidianas que podamos imaginar.

UN POCO DE HISTORIA

Para entender qué es la criptografía primero debemos saber de dónde proviene o donde se originó. Comunicarse de forma secreta a través de la ocultación de un mensaje se conoce como esteganografía, derivado de las palabras στεγανο(steganpos), que significa encubierto, y γραπτοζ (gráphos), que significa escritura. Un ejemplo de esto lo encontramos en la antigua China donde escribían mensajes en seda fina que luego aplastaban hasta crear una pequeña bolita que era cubierta de cera, la cual posteriormente ingería el portador del mensaje y el resto todos sabemos cómo acaba.

Este método ha llegado hasta nuestros días y es usado por traficantes para portar sustancias ilegales. Con la llegada de los ordenadores se pasó a ocultar mensajes en contenidos multimedia, mezclando bits del mensaje original entre los bits del archivo, pero con la sofisticación de la tecnología, alguien concienzudo sería capaz de averiguarlos por lo que comenzó el estudio de la criptografía.

La criptología procede del griego krypto y logos, que significa el estudio de lo oculto, lo escondido, y dentro de esta encontramos dos ramas, la criptografía y el criptoanálisis. En el presente artículo nos centraremos en la criptografía, que es la disciplina encarga de esconder, ocultar, hacer inteligible el mensaje que queramos compartir entre personas, mediante un procedimiento que se conoce como cifrar. En contraposición tenemos a la otra rama de la criptología, el criptoanálisis, el cual se trata de romper ese cifrado para recuperar la información oculta.

Antiguamente, como hemos comentado, la criptografía se usaba principalmente para mantener mensajes importantes ocultos a terceros, sobre todo en tiempos de guerra, pero actualmente tiene otros propósitos:

- Que el mensaje sea confidencial, es decir, que solo puedan acceder a él las personas que estén autorizadas para ello.
- Que se garantice la autenticidad tanto del destinatario como del remitente, es decir, comprobar la identidad de ambos.
- Que el mensaje llegue íntegramente al receptor, es decir, que el mensaje enviado por A sea el mismo que recibe B.

TÉRMINOS Y CURIOSIDADES

A continuación, vamos a comentar algunos términos que serán de gran utilidad a la hora de comprender mejor cómo funciona esto de la criptografía.
Para comenzar tenemos que saber que existen dos métodos de criptográficos dependiendo del tipo de clave que se utilice:

❖ Sistema de clave privada o método simétrico, son los métodos que utilizan una única clave tanto para cifrar como para descifrar el mensaje.
❖ Sistemas de clave pública o asimétrica, se tratan de métodos en los que los procesos de cifrar y descifrar se llevan a cabo con dos claves, una pública y una privada, las cuales son complementarias.

Dentro del cifrado simétrico encontramos dos tipos de algoritmos:

❖ Cifrado en bloque: consiste en cifrar el mensaje original agrupándolo en bloques de un tamaño determinado, por ejemplo 128 bits.
❖ Cifrado en flujo: consiste en cifrar el mensaje original bit a bit o byte a byte.

Dentro del cifrado de clave pública o asimétrica encontramos dos métodos:

❖ Cifrado por sustitución: consiste en ir sustituyendo cada letra del alfabeto en el que está escrito el mensaje que queremos enviar y los elementos de otro alfabeto pudiendo ser el mismo o no.
❖ Cifrado por transposición: se trata de reorganizar las letras del texto claro y colocarlas en una posición distinta, de esta forma, el mensaje cifrado contiene los mismos caracteres que el mensaje original, pero en distinta posición.

Estos dos métodos de cifrado eran usados en la criptografía clásica, ya que actualmente, casi cualquier persona, en un periodo de tiempo relativamente corto, podría obtener un mensaje original que esté cifrado por sustitución o transposición.

IMPORTANCIA HOY EN DÍA EN LA CIBERSEGURIDAD

Como hemos visto, la criptografía se ha utilizado desde hace miles de años, y actualmente está cada vez más presente en nuestro día a día, aunque la mayoría de las veces no nos damos cuenta. Esto ocurre por ejemplo cuando compramos a través de internet y pagamos con nuestra tarjeta del banco. Por ejemplo, cuando accedemos a nuestro correo electrónico, a través del navegador podemos encontrar un candadito en la parte superior de la barra del dominio, esto quiere decir que estamos navegando por una página cifrada, pero esto tampoco quiere decir que estemos enviando la información a la persona que deseamos, ya que alguien ha podido interponerse entre nosotros y el destinatario y recibir la información.

La criptografía también está presente cuando realizamos acciones con la Administración Pública, a través de la firma o el DNI electrónicos.

En la simple acción de mandarnos mensajes a través de la conocida app WhatsApp estamos haciendo uso de la criptografía ya que las comunicaciones están cifradas de extremo a extremo, este tipo de cifrado garantiza que solo tú y la persona con la que te estás comunicando podáis leer o escuchar lo que estáis enviando y ni siquiera WhatsApp tiene acceso a esa información.

Como podemos deducir la criptografía es también una herramienta muy importante en el ámbito de la ciberseguridad. Actualmente la mayoría de los trabajos están industrializados e informatizados de alguna forma, lo que conlleva un aumento del riesgo de sufrir ciberataques, por ello, el uso de la criptografía sobre las comunicaciones o sobre los dispositivos que se utilizan en las empresas es una medida extra de seguridad que siempre puede reducir los ataques.

Por ejemplo, existen certificados para la autenticación de los dispositivos a través de los cuales seremos capaces de saber quiénes están detrás de cada dispositivo que hay conectado a nuestra red y así poder evitar amenazas.

CONCLUSIONES

En un mundo prácticamente informatizado, en el que los principales activos de las empresas y de las personas son la información, ya sea privada, como datos bancarios o información confidencial como estrategias de mercado, necesitamos de la criptografía junto con la ciberseguridad para que las comunicaciones y el traspaso de información sea lo más seguro posible y no existan intermediarios que intenten acceder a ella o directamente robarla.

Autora: Janira Pérez Sánchez. Criminóloga. Colaboradora en el área de Ciberseguridad en Sec2Crime

El Día de la Hispanidad: Desfile del 12 de Octubre

Celebrar el 12 de octubre no solo supone la conmemoración de un hecho importante en la historia de España, sino que busca realzar la presencia, el trabajo y el compromiso del Ejército español y el conjunto de las Fuerzas Armadas.

INTRODUCCIÓN

Sin dejar de tener en cuenta el trabajo discreto de los militares que llevan a cabo en territorio nacional y extranjero, estos dos últimos años han sucedido en España y en el resto del mundo hechos históricos que han marcado un antes y un después en nuestras vidas, y el Ejército español ha estado presente cuidando y protegiendo a cada uno de los ciudadanos españoles sin pedir nada a cambio

La operación Balmis, que desplegó a mas de 2.500 efectivos del Ejército delAire, del Ejército de Tierra, de la Armada, de la UME (Unidad Militar de Emergencias) y del a Guardia Real por toda España para poder hacer frente al Coronavirus; la operación NEO (Non-Combatant Evacuation Operation) de Afganistán, coincidente con la toma de poder de los Talibán en Afganistán, en la que las Fuerzas Armadas evacuaron a más de 2.000 personas desde el aeropuerto de Kabul;los trabajos durante la nevada de Filomena con más de 1.500 efectivos de la UME, del Ejército de Tierra y del Ejército del Aire, que facilitaron la movilidad y las vidas de todos los ciudadanos afectados; y la más reciente, el despliegue de 184 efectivos de la UME y del Ejército del Aire para evacuar y apoyar a los ciudadanos afectados por la erupción del volcán Cumbre Vieja en La Palma (Islas Canarias).

.

Las Fuerzas Armadas han estado a nuestro lado todo este tiempo, como lo hacen diariamente, y el desfile del 12 de octurbe es un acto de visualización, celebración y agradecimiento a su dedicación y a su servicio.

QUÉ ES EL 12 DE OCTUBRE, LA FIESTA NACIONAL DE ESPAÑA

Desde su origen hasta nuestros días, exceptuando el año de la pandemia del Coronavirus (2020) que impidió su celebración tal y como la conocemos, el día de la Hispanidad se ha celebrado como uno de los eventos más importantes para España y para todos los españoles. También conocido como el día Nacional de España, coincide a su vez con el Día de La Virgen del Pilar, patrona de Aragón, y de su capital, Zaragoza.

El 12 de octubre de 1492 Cristóbal Colón pisó América por primera vez, un acontecimiento que dio lugar a la conexión del mundo que se conocía hasta entonces y aquel "nuevo mundo". En 1913, Faustino Rodríguez San Pedro, abogado y político español, propone desde la Organización Ibero-Americana la celebración del 12 de octubre como Fiesta de la Raza Española y en 1918 esta fecha se convierte en día festivo bajo el Gobierno Nacional de Antonio Maura, presidente del Partido Liberal-Conservador entre 1918 y 1922. Su término oficial entra en vigor en 1987 con la Ley 18/1987 del BOE (Boletín Oficial del Estado) que establece el Día de la Fiesta Nacional de España el 12 de octubre.

¿POR QUÉ SE CELEBRA Y POR QUÉ ES IMPORTANTE EL DESFILE?

Celebrar el 12 de octubre no solo supone la conmemoración de un hecho importante en la historia de España y del mundo que forma parte del patrimonio cultural, histórico y social de los ciudadanos españoles, sino que busca realzar la presencia, el trabajo, el compromiso, la profesionalidad, la modernidad y todas las virtudes del Ejército español y el conjunto de las Fuerzas Armadas que trabajan diariamente en el bienestar de toda la ciudadanía española y la defensa de España.

La conmemoración de este acto es de toda la sociedad española ya que, para la íntegra y holística defensa de España, no solo han de estar al mando las Fuerzas Armadas y los Cuerpos de Seguridad del Estado, que son una parte fundamental, sino que todo el conjunto de la sociedad civil debe tener conocimiento y saber qué es el Ejército, qué cuerpos lo forman o cómo trabajan.

El 12 de octubre es un acto de visualización y de reconocimiento que nos permite apreciar cómo está formado el Ejército y, por supuesto, un acto de cultura y concienciación de la Defensa que cada año rinde homenaje a los que dieron su vida por España.

EL DESFILE Y SUS PARTICIPANTES:

Más de 4.000 miembros, tanto de tierra como de aire, recorren cada año el Paseo de la Castellana de Madrid en la ceremonia militar presidida por los SS.MM los Reyes de España.

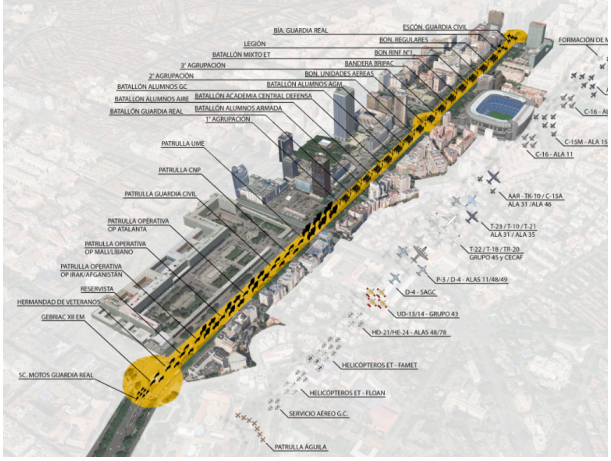
Una vez ha sonado el Himno de España y SS.MM saluda a las autoridades, el JEMAD (Jefe del Estado Mayor de la Defensa) pide permiso para dar comienzo a los actos y, a continuación, un miembro de la Brigada Paracaidista del Ejército del Aire realiza un salto con la bandera nacional española.

Minutos después, miembros del Ejército de Tierra, la Armada, el Ejército del Aire, la Guardia Civil y la Policía Nacional izan la bandera y se celebra el homenaje a la bandera nacional y a todos los que murieron por su Patria.

El Ejército del Aire es el primero en desfilar con diferentes aeronaves devigilancia marina y aduanera, hidroaviones, cazas y helicópteros de diferentes cuerpos y es la Patrulla Águila la encargada de cerrar este desfile con su característico trazados formando la bandera de España en el cielo.

A continuación, comienza el Desfile Terrestre con las motos de la Guardia Real, la Hermandad de Veteranos de la Guardia Civil, La Legión y la Armada. Les siguen los reservistas, diferentes patrullas operativas y las patrullas de la Guardia Civil, la UME y el Cuerpo Nacional de Policía, diversos Batallones, la Brigada Paracaidista y La Legión, cerrando el Desfile la Guardia Real y la Guardia Civil.

Para finalizar, se realiza el saludo de SS.MM los Reyes a autoridades militares participantes en el desfile y la despedida.



Esquema de los participantes en el desfile del 12 de octubre. Fuente: 20 minutos

Edurne Villanueva, investigadora de la UNINT (Unidad de Análisis de Inteligencia) de la Universidad Autónoma de Madrid.

La Criminalidad de Cuello Blanco Femenina en Cifras

La Delincuencia de Cuello Blanco es una categoría delictiva para la que la investigación está en auge. Con el paso de los años la respuesta social y penal es cada vez mayor, provocando un rechazo al delito que no se aprecia en tiempos anteriores. Las mujeres, aunque en menor medida que los hombres, también son autoras de modalidades delictivas encuadrables en DCB.

Lo que se pretende en las siguientes líneas es plasmar los datos de la criminalidad femenina, las posibles interpretaciones de los mismos para dejar una puerta abierta a la futura investigación más profunda en la que se demuestre los motivos de las diferencias de cifras, si estas se deben a una desigualdad social, delictual, mayor permisibilidad.

De forma que la criminalidad femenina y los delitos de cuello blanco se representan en cifras para comprender con mayor facilidad el fenómeno.

Es imposible valorar las cifras de mujeres condenas sin contraponer los datos que corresponden a sexo hombre para hacer esta valoración. Probado está, a la luz de los datos, que las mujeres cometen menos delitos que los hombres, pero este no es el momento de crítica al sistema judicial actual por intuir una mayor permisividad al delito de las mujeres dejándolas sin condena, o peor aún, una mayor facilidad para encubrir el delito y no ser descubiertas pues se carecen de pruebas para esto.

En el plano de lo real, solo podemos manejar y analizar los datos de fuentes y organismos oficiales, pues son los que aportan una mayor seguridad. Es inevitable pensar que, para la delincuencia de cuello blanco, las cifras se van a reproducir de forma sistemática y que habrá una menor tasa de delincuencia femenina, una menor tasa de condenas y por tanto una menor tasa de encarceladas y así lo presentan los datos facilitados por el INE en relación con los años 2019, 2018 y 2017 de manera que no estamos ante un ideario, es una realidad que para los delitos de cuello blanco, las mujeres también delinquen menos.

En España el delito de blanqueo de capitales y receptación es el delito tipo “base” para el supuesto de la delincuencia de cuello blanco (es el ejemplo primigenio del que se extraen con facilidad cada uno de los elementos diferenciadores), que de forma mas o menos uniforme se acompaña de otros como las falsedades en documentos o la apropiación indebida. Cierto es que no son tipos automática y únicamente aplicables a esto, pero si de forma generalizada y primordial se producen por las dificultades que se presentan para realizarse fuera de esta esfera.

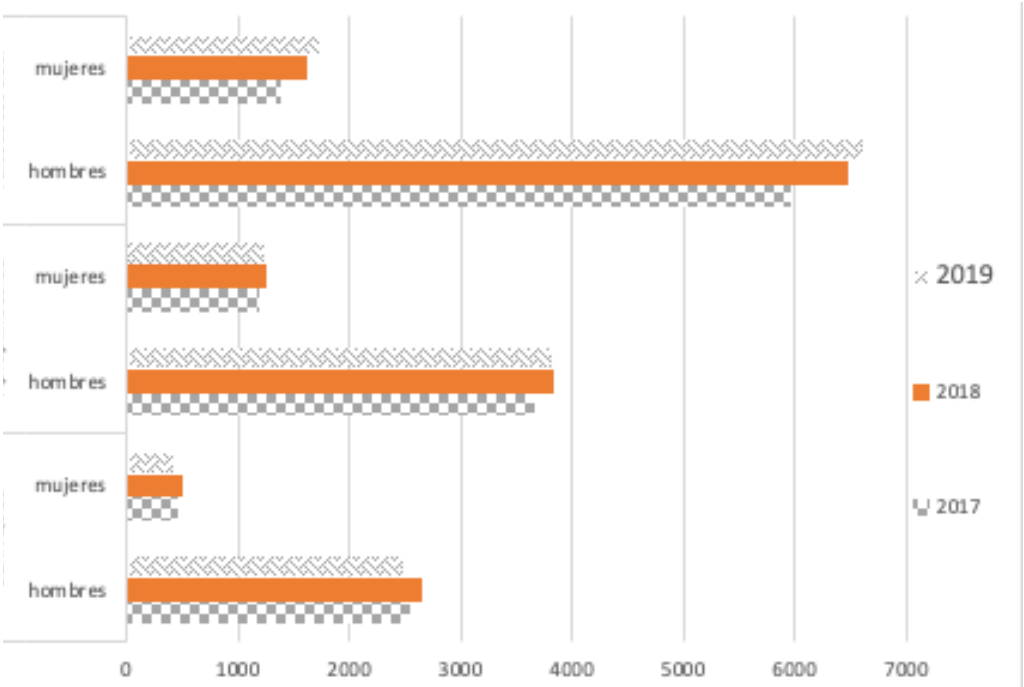
Extrapolando los datos de la gráfica, de nuevo aparece irremediablemente una menor tasa en el caso de las mujeres, que en el supuesto de los hombres para las tres modalidades de delitos y para los tres años de forma consecutiva.

En el blanqueo de capitales, las mujeres presentan cifras homogéneas durante los tres años, 471 casos en 2017, 496 en 2018 y 442 en 2019. En contraposición, en 2017 fueron condenados 2550 hombres, 2665 en 2018 y 2494 en 2019.

Hay en uno y otro caso un incremento de condenas en el 2018, que disminuye de nuevo en 2019 por debajo de las cifras de 2017, lo que no presentan relevancia. Hay que apelar también a que estos delitos van acompañados de largos procesos judiciales, lo que innegablemente puede suponer una acumulación de condenas, teniendo así mismo claro que no son delitos comunes. La tendencia a la baja de cifras, igualmente se puede deber a la relajación del esclarecimiento delictivo, trasladando el foco a otras tipologías.

Lo que no se puede discutir es que mas mujeres representan en los tres años, de forma aproximada y generalizando un 15% de las condenas por delitos de cuello (85% hombres), mientras que en relación con la totalidad delictiva que se condenó en España representan un 19,5% aproximadamente en 2019, y un 19,6% en 2018.

La incidencia de la delincuencia femenina para los delitos acomodados en la categoría "de cuello blanco", es muy significativamente menor a la de los hombres y menor a la del resto de delitos. Ya la discusión se deriva hacía el motivo, no de la menor criminalidad femenina, sino hacia el caso concreto de la delincuencia de cuello blanco para la que los porcentajes caen alrededor de un 4,5. Es momento de preguntarse, por tanto, cual es la causa, por el que aún las mujeres delinquen menos en los casos de cuello blanco. Visualizando la gráfica creada al efecto en la que únicamente se contemplan los datos de blanqueo de capitales y receptación se apela a una oposición abismal, para la que en 2019 se aprecia una diferencia de 2050 casos entre hombres y mujeres.



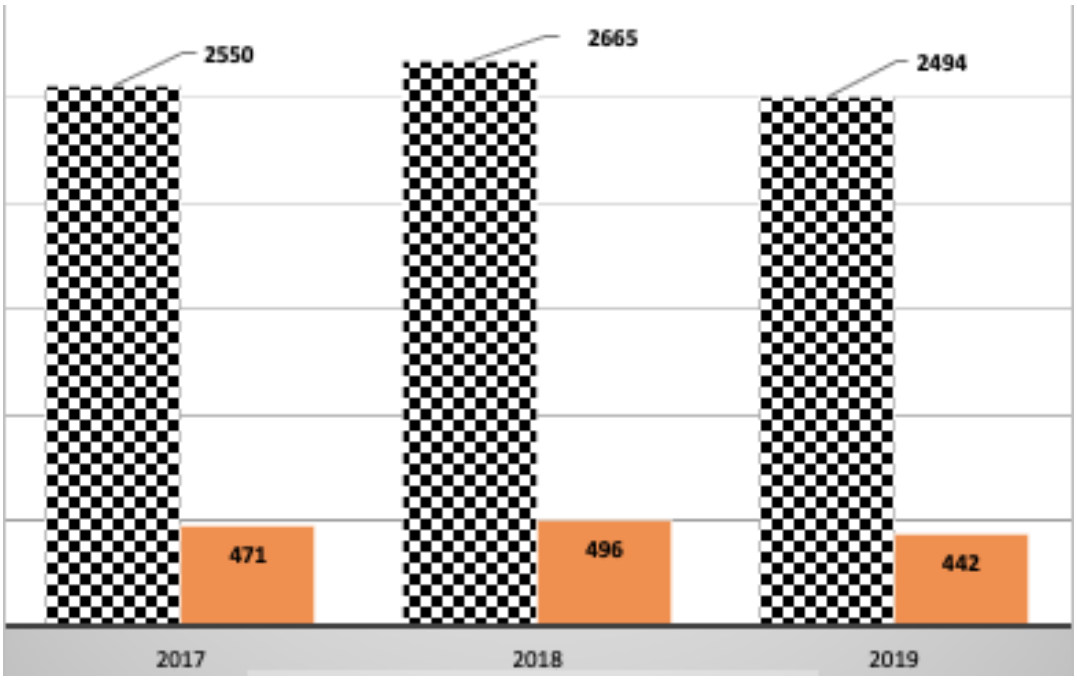
Llegado el caso, solo queda concluir los motivos por los que estos porcentajes son tan diferentes; se puede tratar de una simple coincidencia con las cifras que se presentan para el resto de los delitos y que debamos asumir que las mujeres delinquen menos que los hombres, se puede tratar también del caso de la excusa absolutoria contemplada en el Código Penal o bien porque las mujeres no acceden a los puestos que las facilitarían la comisión de estos delitos.

Antes de asumir la coincidencia y no darle más importancia la diferencia de cifras o tener claro que bien las mujeres delinquen menos o que estas son descubiertas en menor medida, lo que puede ser un indicador más pero no el único de las diferencias. Hay que apreciar, los datos de los que se disponen, en cuanto a mujeres en puestos de poder, que las ubiquen en una posición para que sea posible que cometan dichos delitos.

Según el Informe Women In Business 2020 las mujeres españolas representan un 38% de los puestos de poder, frente al 62% de los hombres; lo que es una guía de que las mujeres aparecen en los puestos de poner menos que los hombres.

Una de las hipótesis- motivos por lo que las mujeres delinquen menos que los hombres en el caso de la criminalidad de cuello blanco, es por su dificultad para llegar a esos puestos de poder, en lo que además de llegar menos y con mayores dificultades se las exige mayores requisitos que a los hombres, sometidas a diferentes controles y valoraciones.

El otro de los motivos que podemos juzgar, son las excusas absolutorias, las cuales no tienen demasiado sentido cuando se trata de valorar está criminalidad como sujeto activo principal del delito.



Estas escusas se suelen utilizar cuando se juzga a un delincuente de cuello blanco y su pareja forma parte del proceso por encubrimiento o por colaboración en los delitos de – principalmente – sus maridos.

CONCLUSIONES

Claramente la mujer es menos criminal que el hombre. No podemos amparar una afirmación contraria en hipótesis o sugestiones, en la manera que solo se han podido discutir los datos ofrecidos por organismos oficiales y hechos probados.

A lo largo de la historia la criminalidad ha sido objeto de estudio desde distintas perspectivas, pero siempre enfocada a la pobreza y la masculinidad, dejando que la criminalidad femenina en muchas ocasiones fuera juzgada en casa.

Esto ha supuesto un abandono a nuevas perspectivas delictuales y ha provocado la deriva de los estudios y de las investigaciones hasta tal punto de olvidarse de la criminalidad más rica y de la femenina.

Que la tasa de criminalidad femenina sea inferior, se debe a que delinquen menos que los hombres y/o el esclarecimiento de los delitos es menor, que existe un uso abusivo de excusas absolutorias, principalmente y para el caso que compete en estas páginas es la dificultad de las mujeres en obtener un puesto de control. Es aquí donde está el punto del que se debe partir, la desigualdad latente que existe en el ámbito laboral, la misma que provoca que el número de mujeres en puestos de responsabilidad sea menor, lo que se acompaña de un examen exhaustivo a su labor, dificultando indudablemente la comisión delictiva.

Deriva, por tanto, que un mayor control generalizado disminuiría las tasas de delincuencia de cuello blanco también para los hombres, a lo que habría que añadir otras variables.

La desigualdad de la mujer en el ámbito social y laboral repercute en las tasas de delincuencia causando una disminución de la criminalidad. Esto nos hace preguntarnos que ocurrirá cuando la participación de la mujer en la vida laboral, social, cultural…sea en plena igualdad a la del hombre, si aumentará la criminalidad femenina o se mantendrá en las mismas tasas, pues a pesar de que la mujer está cada vez más presente en todos los ámbitos la criminalidad sigue siendo mucho menor, lo que no impide abogar por la educación en igualdad y en valores que disminuyan las cifras de criminalidad a tasas más tolerables lo que también se debe acompañar por mayores controles y más exhaustivos.

Autora: Alicia Rodríguez Sánchez. Criminóloga y Personal Investigador USAL.

Las Apuestas y el Blanqueo de Capitales

¿QUÉ HACE DE LAS APUESTAS UN BUEN CANAL PARA BLANQUEAR DINERO?

En primer lugar, cabe destacar que cualquier actividad que oscurezca la fuente original de ciertos fondos plantea un cierto riesgo en materia de blanqueo de capitales. Y en la industria del gambling este riesgo es muy notable, desde las apuestas más tradicionales en casinos o maquinas de apuestas hasta la ascendente tendencia de las apuestas online.
El usuario dispone de diversas formas de transferir el dinero a las cuentas desde las que después se realizarán las apuestas. Se puede hacer desde una cuenta bancaria (la opción que menos riesgo conlleva) pero también existen otras opciones, muchas de las cuales tienen la cualidad de ocultar de donde provienen esos fondos. Por ejemplo, tarjetas prepago, debito, cheques, dinero en efectivo o incluso criptomonedas

Los modus operandi más habituales y explicativos de como este sector puede plantear un alto riesgo son los siguientes: alguien abre una cuenta en un proveedor de servicios de apuestas online, y aunque habitualmente se requiere proveer una cuenta bancaria para abrir la cuenta de gambling, una vez abierta no necesariamente se van a transferir los pagos desde ésta, ya que existen diversas opciones de pago como hemos explicado anteriormente. .

Después de introducir el dinero oscureciendo su origen hay dos opciones:

- Puede que el usuario no utilice ese dinero para apostar (o únicamente de forma residual), y simplemente lo tenga allí depositado para ocultarlo a las autoridades y sacarlo cuando sea conveniente de forma que está 'lavando' el dinero al hacer ver que viene de una fuente aparentemente legítima.

- O bien, de forma más elaborada, se puede utilizar el dinero para apostar, amañando partidas con otros jugadores en juegos como el póker online por ejemplo, de forma que múltiples jugadores pueden trabajar de forma conjunta para darle a ese dinero una mayor apariencia de legalidad.

Una tercera opción, en los proveedores de servicios que lo permiten, es utilizar estos fondos ya ingresados en una cuenta de gambling para enviar fondos a otros jugadores. Por lo que funcionarían en todos los aspectos como una cuenta bancaria, pudiendo oscurecer los beneficios por las ventas de un producto (en ocasiones productos restringidos o ilegales) mientras que el beneficiario de estos fondos podría alegar al retirarlos que provienen de ganancias en forma de apuestas.

LEGISLACIÓN EUROPEA Y ESPAÑOLA RESPECTO A LOS JUEGOS DE AZAR

Los casinos han sido considerados sujetos obligados desde la promulgación de la Ley 19/1993, sobre determinadas medidas de prevención del blanqueo de capitales. Con la cuarta directiva europea en materia de blanqueo vemos que Europa comienza a contemplar otros operadores de juego distintos de los casinos con el término "servicios de juego". El legislador europeo los define como servicios que "impliquen apuestas de valor monetario en juegos de azar, incluidos aquellos con un componente de habilidad como las loterías, los juegos de casino, el póquer y las apuestas, y que se preste en una ubicación física, o por cualquier medio a distancia, por medios electrónicos o mediante cualquier otra tecnología que facilite la comunicación, y a petición individual del destinatario del servicio".

Además, la Cuarta Directiva permite eximir total o parcialmente a determinados proveedores de servicios de juegos de azar, a excepción de los casinos, cuando exista un bajo riesgo por la dimensión de las operaciones de tales servicios.

Podemos observar que, si bien existe regulación al respecto, se sigue considerando ampliamente insuficiente, sobretodo debido al rápido desarrollo que ha experimentado la industria en materia de apuestas online.

PREVENCIÓN, REQUERIMIENTOS FUNDAMENTALES

Es cierto que los riesgos que plantea esta industria se pueden mitigar de diversas formas:

- Teniendo un sólido programa de Compliance / AML, que indique como se compromete el proveedor de servicios de apuestas a detectar, analizar y reportar ante las autoridades incidentes que sean sospechosos de ser blanqueo de capitales o fraude. Éste tiene que ser un programa específicamente diseñado para su modelo de negocio en particular.

- Medidas de diligencia debida (due dilligence). Con esto nos referimos a identificar quién es el cliente con el que se está tratando antes de permitirle usar tales servicios, asegurando que no plantea un riesgo elevado de blanqueo de capitales u otros delitos económicos. Esto requiere identificar y verificar la identidad del cliente para hacer una investigación adecuada (screening) y compararlo ante bases de datos para comprobar que no es una persona sancionada o incluida en alguna lista negra (blacklists) así como identificar si estamos tratando con un PEP, también conocido como persona políticamente expuesta.

- Entrenando al personal en el conocimiento de las políticas de prevención de blanqueo de capitales y la detección de red flags.

- Reportando a las autoridades siempre que haya sospecha de actividad ilegal.

CONCLUSIONES

En conclusión, el sector de las apuestas es muy atractivo para aquellos individuos que buscan blanquear dinero porque existen varios métodos de pago que anonimizan el origen de los fondos que se van a utilizar, dificultando la detección de red flags (principalmente en la industria del gambling online). Las transferencias de dinero son muy frecuentemente internacionales, lo cual dificulta su investigación. Y finalmente, no requiere de ningún bien físico que pueda dar testimonio de donde se han generado los fondos, lo cual ayuda a oscurecer en mayor medida el origen de los mismos.

BIBLIOGRAFÍA

- Carlavilla, J. (2020, 26 noviembre).Casinos y juegos de azar en la prevención del blanqueo de capitales – Pibisi. Pibisi. https://blog.pibisi.com/es/2020/11/casinos-y-juegos-de-azar-en-la-prevencion-del-blanqueo-de-capitales/
- Vlada, I. (2021, 10 junio).A Complete Guide to Casino Compliance: AML, Responsible Gambling, and Data Protection. Sumsub. https://sumsub.com/blog/a-complete-guide-to-casino-compliance-aml-responsible-gambling-and-data-protection/
- Boere, N. (2021, 8 enero).Online gambling as a money laundering method. AMLC.EU. https://www.amlc.eu/online-gambling-as-a-money-laundering-method/
- Kask, J. (2021, 13 agosto).Guide: Anti-Money Laundering in Gambling. Roaring.Io. https://www.roaring.io/en/guide-aml-gambling/

Autor: *Borja Ferrer Comes. Criminólogo, KYC/AML Analyst en Ebury y colaborador en el área de Delincuencia Económica de Sec2Crime.*

Entendiendo la Violencia Yihadista

Resumen: ¿En que consiste la violencia yihadista? ¿Qué relación guarda con el "conflicto"? ¿Se considera esta un tipo de "agresión"? La presente pieza de estudio plantea nuevos enfoques acerca de lo que se entiende por "violencia yihadista" desde una perspectiva psicosocial. Así pues, se niega la posible existencia de una "violencia yihadista nihilista" o ultraviolencia.Por otro lado, el auto-esteriotipado y el autoanclaje explican en qué medida se puede calificar la violencia yihadista de "violencia intergrupal", independientemente de que esta sea cometida por un terrorista autónomo. ¿Cuáles es su origen? ¿Se trata de un aprendizaje cultural o social? Siga leyendo.

Palabras clave: Violencia, Agresión, Conflicto, Yihadista, Intergrupal, Social y Cultural.

¿QUÉ ES LA VIOLENCIA YIHADISTA?

Violencia, agresión y conflicto son términos que se suelen utilizar de manera intercambiable. El conflicto es una acción que deriva de una incompatibilidad de objetivos, metas o intereses de los partícipes del mismo. El conflicto en sí es el resultado conductual de un individuo que utiliza protestas, represalias o una oposición mediante sus actuaciones con el fin de alcanzar sus intereses frente a los de otro.

El conflicto puede ser constructivo o destructivo. 1 De este modo es importante destacar que el conflicto no está ligado necesariamente a la agresión. 2 Los conflictos denotan una connotación positiva debido a la posibilidad que otorgan de enriquecer las elaciones sin necesidad de establecer vencedores ni vencidos.

A diferencia del conflicto, la agresión tiene como objetivo dañar. La psicología social entiende por agresión aquel conjunto de conductas que sin provocación previa buscan generar un daño, indiferentemente de sus intereses, metas u objetivos

De este modo las agresiones por ende revelan una visión negativa y destructiva. 3 En un caso típico de agresión se dan tres características: intención de causar daño, provocar un daño real y la existencia de una alteración del estado emocional del sujeto.

Existen tres tipos de agresión: la agresión colérica fruto de una provocación previa que tendría como objetivo generar un daño, la instrumental la cual no tiene como objetivo dañar (pero existe la posibilidad de contemplarla como un "mal menor" 4 necesario) y estaría orientada a utilizar la misma en beneficio propio con el fin de defenderse o aventajarse. Y por último la agresión social, la cual tiene como objetivo dañar la autoestima, relaciones o estatus de una persona.

De este modo, existe una clara diferencia entre agresión y conflicto, el conflicto utiliza la violencia como medio y la agresión como un fin en sí misma (con matices respecto a la instrumental). Sin embargo no existe diferencia alguna entre lo que se entiende por agresión y violencia ya que ambas tienen como finalidad dañar. Algunas definiciones contemplan la violencia como un tipo de agresión.

La definición más empleada a día de hoy es la otorgada por la UNESCO: "todo cuanto se encamine a conseguir algo mediante el empleo de una fuerza, a menudo física, que anula la voluntad del otro" concepto que la aproxima más al conflicto. Desde una perspectiva psicológica y social se entiende por violencia "aquellas conductas con tendencia hostil o destructiva" lo que la aleja del conflicto y la acerca a la agresión. 5

Como podemos comprobar existe una disparidad de ideas acerca de la violencia yihadista ¿Es un terminó cercano al conflicto o guarda mayor relación con la agresión? Lo cierto es que esta violencia es un producto de ambas. Lo es de conflicto porque es utilizada como un medio para alcanzar unos fines, cosa que no sucede en los casos de violencia nihilista donde en un fin en sí misma. 6 Y lo es de la agresión por su connotación negativa y destructiva. De este modo podemos definir la violencia yihadista como una modalidad de violencia que se emplea en contextos dónde existe un conflicto de intereses y tiene una finalidad destructiva.

En la actualidad se ha abierto un nuevo debate acerca de la violencia yihadista. Existen quienes defienden el concepto de violencia nihilista yihadista (ultraviolencia) 7 como un fin en contraposición a los que la definen como un medio (violencia instrumental).
Hablar de violencia yihadista como fin sería asociar esta violencia al nihilismo y por ende supondría asumir la "no" existencia de un conflicto (en este caso de valores).

Las sociedades actuales contemplan dos modalidades de violencia; la normal, concebid como residual y la ultraviolencia (nihilista). La ultraviolencia se caracteriza en que lejos de ser un instrumento se convierte en un fin en sí mismo.

En cuanto a la violencia yihadista resulta evidente que se trata de una violencia instrumental o residual. Los deseos de alteración de un orden para sustituirlo por otro acompañada de una ética moral justificada por unos valores legitimizadores tienen una finalidad clara que legitimiza su uso. Federico Aznar ejemplifica muy bien el concepto de violencia yihadista cuando comenta:" la violencia es un suplemento de los conflictos, no su esencia."

Por lo que en el caso del yihadismo el nihilismo es inconcebible ya que su arraigo a determinados valores impiden dicha connotación. En todo caso sería en la sociedad occidental donde adquiriría dicho matiz lo que tampoco es coherente al proceso de transvaloración actual en el que nos encontramos.

TIPO DE VIOLENCIA: ¿INTERDIVIDUAL O INTERGRUPAL?

A Existen dos tipos de violencia, la interindividual y la intergrupal. 10 Un ejemplo práctico de esta última sería la originada entre dos grupos rivales (endogrupo vs exogrupo) como podrían ser diferentes pandillas y en cuanto a la interindividual la originada entre dos individuos aislados de un grupo.

Sin embargo existen propuestas que hablan de actos tales como la agresión de un grupo a un individuo o la de un individuo a un grupo. Claros ejemplos de ello los encontraríamos en el terrorismo yihadista donde puede producirse tanto la actuación de un autor individual frente a un grupo o la de un grupo terrorista frente a una autoridad social relevante. Ambas acciones dentro de la psicología social se encontrarían enmarcada en violencia intergrupal.

La primera porque a pesar de ser un individuo concreto pertenece a un grupo y la segunda por que dicha autoridad se mostraría como figura representativa de otrocolectivo. 11 Por lo tanto la violencia yihadista es un tipo de violencia intergrupal que presenta diferentes variables.

Estudios focalizados en las "Superposiciones de representaciones mentales de uno mismo" han demostrado el modo en el que uno mismo se define en términos de su grupo. Existen dos formas de que uno se vea representado por el grupo, el auto-esteriotipado y el autoanclaje. 12 En el primero se producen inferencias del grupo al yo, (sentimiento de pertenencia) mientras que el en segundo ocurre lo contrario, existen más inferencias de uno mismo al grupo (inspiración). Por ello, indiferentemente de cómo se cree el vínculo entre el yo y el endogrupo, existe una
correlación que une al yihadista con este, y del mismo modo a la víctima con la sociedad a la que pertenece o se inspira (exogrupo).

ORIGEN Y TRASMISIÓN DE LA VIOLENCIA

Desde una perspectiva psicológica la violencia se originaria a causa de antecedentes situacionales, motivacionales o socio-motivacionales. Entre los antecedentes situacionales diferenciaríamos entre: los causados por una agresión o los producidos por estímulos físicos o ambientales. En relación con los motivacionales o socio motivacionales podemos distinguir entre: los de fustración-agresión, los emocionales (colera e ira), los ataques interpersonales o provocaciones, los de sentimiento de rechazo, o los relacionados con la violación de normas. 13

En cuanto a su transmisión podemos distinguir entre "el aprendizaje social" o "aprendizaje cultural". El aprendizaje social es un modelo conductual por el cual el individuo se desarrolla siendo la agresividad una de sus posibles manifestaciones. Es relevante matizar la importancia del modelo para el observador así como lo relativo a

Sin embargo, el aprendizaje cultural está ligado a los valores y normas de una sociedad determinada. Debido a ello en numerosas ocasiones un análisis de normativo y de valores culturales sirve como un predictor veraz de la violencia. 15

Es por esto que los valores del islam interpretados de manera extrema originan violencia. La violencia yihadista se desarrolla bajo un aprendizaje cultural, 16 el cual no sería posible sin los mecanismos de socialización desde donde se traspasan, 17 por lo que el aprendizaje social actuaría a su vez como medio necesario para la adopción de conductas violentas. 18

BIBLIOGRAFÍA

1 Los conflictos, en muchas ocasiones, pueden propiciar cambios positivos. Para ello es necesario que se gestionen correctamente. Es importante entender que hacer un diagnóstico correcto del conflicto va a determinar el éxito en la resolución de las distintas problemáticas. Si abordamos un conflicto de tipo intergrupal o interindividual como si fuese un conflicto intraindividual, las posibilidades de éxito pueden ser escasas.

2 Gaviria, E. (2006). Conflicto y estrategias de solución. En Á. Gómez; E. Gaviria, e I Fernández, Psicología Social, (pp. 449-4498). Madrid. Sanz y Torres.

3 Morales, J. F. y Arias, A. V. (1999). Agresión. En J. F. Morales y C. Huici (Coords.). Psicología Social (pp. 119-130). Madrid. McGraw-Hill.

4 La Doctrina del Mal Menor define como moralmente válida la elección de la opción que genera un daño en un entorno en el cual no es posible garantizar la beneficencia y se está obligado a actuar. De este modo se reconoce la opción con mal menor como el mayor bien posible.

5 Morales, J. F. y Moya, M. C. (1994). Agresión. En J. F. Morales, M. C. Moya, E .Rebolloso, J. M. Fernández-Dols, C. Huici, J. Marques, D. Páez y J. A. Pérez (Coords), Psicología Social (pp. 465-491). Madrid. McGraw-Hill.

6 Cañete, P (2017). "El yihadismo como expresión de la violencia".Revista del Instituto Español de Estudios Estratégicos. , núm.10. pp. 125-132.

7 Junto a la visión nihilista del yihadismo de Pablo Cañete, aparecen académicos como Crístobal Ortiz, Isaac Caro La yihad sunita del Estado Islámico y Al-Qaeda: islamismo, antiimperialismo… ¿y nihilismo político-mesiánico? Que se postulan en la misma dirección.

8 Aznar Fernández Montesinos, F.(2014) "Reflexiones y debates sobre violencia organizada y economía". Documento de análisis, Instituto Español de Estudios Estratégicos, Consultado:02/03/2020)

9 La transvaloración de todos los valores, concebida ésta como inversión de los valores supremos.

10 Schubert, T., y Otten, S. (2002). Overlap of self, ingroup, and outgroup: Pictorial measures of self-categorization. Self & Identity, 1, 535-576.

11 Lo que se explicaría el concepto de "agencia personal" en la Teoría de la fusión de identidad.

12 Otten S, Epstude K. Representaciones mentales superpuestas de uno mismo, dentro del grupo y fuera del grupo: Desentrañar el autoestereotipo y el autoanclaje. Boletín de Personalidad y Psicología Social . 2006; 32 (7): 957-969. doi: 10.1177 / 0146167206287254

13 Toda esta clasificación la podemos encontrar en: (Arias y Gaviria, 2006; Páez y Ubillos, 2004), donde se analiza a fondo cada una de las tipologías.

14 López-Zafra, E. (2006). El componente cultural de la violencia. En Morales, J. F., Moya, M. C., Gaviria, E. y Cuadrado, I. (Coords). Psicología Social, (pp. 441- 454). Madrid. McGraw-Hill.

15 Arias, A. V. y Gaviria, E. (2006). La psicología social de la agresión. Aportaciones teóricas y empíricas para la aportación psicopedagógica. En Á. Gómez; E. Gaviria, e I. Fernández, Psicología Social, (pp. 393-446). Madrid. Sanz y Torres.

16 El islam es religión, política y cultura.

17 La radicalización se produce en mayor medida a nivel meso. Para más información revisar: Javier, J. (30 de marzo de 2009). Procesos de radicalización yihadista en España. Análisis sociopolítico en tres niveles. Revista de psicología social. Recuperado de: https://www.ugr.es/~jjordan/publicaciones/radicalizacion.pdf

718 Javier, J. (30 de marzo de 2009). Procesos de radicalización yihadista en España…op.cit.,

Autor: Jacobo Salvador Micó Faus. Criminólogo, Analista en Terrorismo e Investigador en Antisemitismo. Miembro de la Cúpula Directiva de Sec2Crime y Coordinador del Área de Terrorismo y Conflictos Armados.

Del tratamiento de la evidencia digital: Cuando el fin justifica los medios

Resumen:
Cualquier acción en el mundo físico deja un rastro, una huella que acredita ese acontecimiento. En un entorno digital, la huella será digital.

La evidencia digital, no es propia del cibercrimen, se extiende a una multiplicidad de delitos y de áreas, entre las cuales están los delitos informáticos y, puede ser usada para acreditar una multiplicidad de circunstancias en otras áreas del derecho como la laboral, familiar, comercial o administrativa.

Por ello, y dado que la revolución tecnológica ha llegado para instalarse en nuestras vidas y hacerlas más sencillas resaltando la labor del hombre, el tratamiento de la evidencia digital cobra relevancia.

Con este trabajo pretendo bosquejar alguno de los múltiples inconvenientes que trae aparejado el mal tratamiento de la evidencia digital, los motivos de aquel comportamiento adoptado por los operadores judiciales como así también sugerir una dinámica aceptable de trabajo en torno a este tipo de rastro.

DE LA EVIDENCIA FÍSICA Y DE LA DIGITAL

La evidencia física es aquella que se puede palpar, por lo tanto puede decirse que se trata de un elemento material relacionado directamente con el hecho investigado.

Dentro de la evidencia física, se encuentra la electrónica que no es igual a la evidencia digital. Son aquellos dispositivos tecnológicos que se usan para almacenar o transmitir datos, como por ejemplo un teléfono celular, una consola de juegos, una computadora de escritorio o portátil, un disco rígido externo o interno y hasta un dron, pueden ser ejemplos de evidencia electrónica.

Por lo tanto, la evidencia digital, será el dato o información que está contenida en esos dispositivos físicos, y es representada o reflejada a través de un texto, imagen estática o dinámica o un sonido, pero que en realidad está compuesta por unos y ceros, o sea números binarios.

En este punto resulta necesario diferenciar los conceptos de data y metadata para arrojar una cabal comprensión de la temática.

Mientras que la data es la información que contiene el archivo, el mensaje en sí, el audio en si, la imagen en sí, la metadata será la información del archivo propiamente dicho, la que podrá consistir en el autor del mismo, la fecha y hora de creación, su tamaño, la computadora usada, la geolocalización, etc.

La evidencia digital es la metadata que en definitiva acredita o corrobora la existencia de la data.

DE LA LITIGACIÓN CON EVIDENCIA DIGITAL

En la actualidad y desde que la mayoría de los dispositivos son inteligentes, no existe prácticamente ámbito en que no tenga cabida la evidencia digital como medio de prueba.

Por ello, los operadores de la justicia, se ven obligados a manipular este tipo de evidencia y por lo general, tienden a actuar temerosos frente a ella y a cometer los peores errores justificando cualquier resultado en contra o a favor del imputado o de las víctimas, distorsionando con su accionar, la naturaleza de la evidencia digital.

No cabe lugar a dudas, que cuando se está frente a un homicidio se practicarán las pericias sobre el cuerpo del occiso y, como consecuencia de ello, el experto forense practicará la autopsia y expondrá sus conclusiones en forma en un informe pericial, lo que más tarde, reproducirá frente al juez en el debate oral y público brindando su testimonio.

O cuando acontece un accidente de tránsito será el perito accidentológico quien se presente en la escena del crimen y luego de efectuar un análisis de los objetos y sujetos involucrados al igual que el médico forense presentará sus conclusiones en el expediente.

Pero, no ocurre lo mismo cuando se trabaja con evidencia digital. ¿Cuál es la razón por la cual se la desnaturaliza hasta el punto de pensar que cualquiera, inclusive el propio juez, puede analizarla sin la intervención de un experto? ¿Qué factores influyen en este desconocimiento? La evidencia digital no es nueva así como el cibercrimen tampoco lo es.

Las primeras legislaciones en la materia se registraron a partir de 1984 con la ley sobre actos de fraude informático de EEUU y en la actualidad el Convenio de Budapest en 2001 como norma referente en materia de cibercriminalidad.

Desde que se conoce la posibilidad de delinquir a través de sistemas informáticos y mediante el uso de tecnología, se sabe de la importancia de la evidencia digital.

Existen normas, protocolos y manuales que nos dicen sobre cómo debe manipular este tipo de prueba, sin embargo en pocos casos se usan.

Una de las características específicas de este tipo de material es la volatilidad, por ello, en general las normas establecen un orden en el que se deben recolectar y sobre todo la forma. En primer, lugar aquella información que vaya a estar disponible durante el menor período de tiempo, o sea, aquella cuya volatilidad sea mayor. Así, de mayor a menor volatilidad encontramos: a) los registros y contenido de la caché; b) la tabla de enrutamiento, caché ARP, tabla de procesos, estadísticas del kernel, memoria; c) la información temporal del sistema; d) la información contenida en los discos; e) los logs del sistema; f) la configuración física y topología de la red.

Se deberá recopilar esa información mediante software o hardware legal, con licencias vigentes y sobre todo no ejecutar programas que modifiquen la fecha y hora de acceso de todos los ficheros del sistema. Estas normas que poco se respetan, contemplan la forma en la que se debe manipular este tipo de material, desde el secuestro, extracción, conservación y análisis del mismo.

Sin embargo a la hora de investigar, juzgar y definitivamente valorar este material, ninguna de estas normas, reglas o protocolos son contemplados por los operadores de la justicia ni sus auxiliares, los que recurren infructuosamente a las leyes, de fondo y procesales, para subsanar el desconocimiento.

DEL TRATAMIENTO ESPECÍFICO DE LA EVIDENCIA DIGITAL

En ésta área rigen por ejemplo desde el año 2002 la RCF 3227 y/o las normas ISO/IEC 27037 del año 2012 e ISO/IEC 27042 del 2015.

Los RFC o Request For Comments, son documentos que recogen propuestas de expertos en una materia concreta con el fin de establecer, por ejemplo, una serie de pautas para llevar a cabo un proceso como la creación de estándares o la implantación de algún protocolo.

Entre los puntos más importantes de la RFC 3227 se destacan los Principios durante la recolección de evidencias:

- Copiar la imagen del sistema tan precisa como sea posible. No significa una captura de pantalla.
- Realizar notas detalladas.
- Minimizar los cambios en la información que se está recolectando.
- Frente a un dilema entre recolección y análisis, elegir primero recolección.
- Recoger la información según el orden de volatilidad (de mayor a menor).
- Tener en cuenta el tipo de dispositivo del que se recoge la información.
-

Además de la RFC 3227:2002, la referencia normativa actual de mayor importancia para el análisis digital forense es la norma de alcance global ISO/IEC 27037:2012, la que se ha usado como base de protocolos y manuales tanto de organismos internacionales como unidades de investigaciones fiscales y policiales.

En resumen, estas normas, proporcionan pautas para el manejo de la evidencia digital sistematizando la identificación, recolección, adquisición y preservación de la misma al implementar procesos diseñados para respetar y salvaguardar la integridad de la evidencia con una metodología que asegura la correcta admisibilidad en procesos legales.

Habla de los tres principios que la gobiernan: la relevancia, la confiabilidad y la suficiencia y proporciona directrices generales para la obtención de pruebas no digitales que pueden ser útiles en la etapa de análisis de la evidencia digital.

Hace referencia puede obtenerse de diferentes tipos de dispositivos digitales, redes, bases de datos, etc; pero siempre se refiere a datos que ya están en formato digital y no abarca la conversión de datos analógicos a formato digital y plantea el concepto de Cadena de Custodia (CoC) conjuntamente con los recaudos mínimos a tener en cuenta como la presencia de un identificador unívoco de la evidencia; quién, cuándo y dónde accede y. cómo es el pasaje de la evidencia de un sitio a otro.

EVIDENCIA QUE SE PUEDE RECOPILAR DIGITALMENTE

Pueden ser recolectados, los documentos de todos los formatos almacenados en nubes, discos externos o internos teléfonos o computadoras, los correos electrónicos, mensajes de texto e instantáneos, transacciones, imágenes e historiales de Internet son ejemplos de información que se puede recopilar de dispositivos electrónicos y usar de manera muy efectiva como evidencia.

Para garantizar los derechos de las partes, la tutela judicial efectiva de la víctima y la garantía de defensa en juicio del victimario o sospechado el proceso debe ser auditable esto es, que todo el procedimiento que se ha seguido para la adquisición de la evidencia digital debe quedar registrado y validado por las buenas prácticas profesionales.

Las evidencias y las trazas de nuestro procedimiento deben estar disponibles para que pueda ser controlada y cotejada por la contraparte. A su vez debe ser reproducible lo que significa que el procedimiento llevado a cabo y todos nuestros métodos deben ser de posible reproducción posterior por los profesionales intervinientes o quienes deban adoptar una decisión o deban dar validez a nuestras actos.

Los procesos ineludibles para poner en práctica son la Identificación de la evidencia, lo que implica localizar e identificar donde está la información potencial, ya sea en estado físico o lógico. Otro proceso de trascendencia es la recolección que debe ser una copia exacta de lo contenido y por último la conservación o preservación de la evidencia, de la cual se deja constancia en una cadena de custodia que asegura la integridad de la misma.

Por otra parte la ISO 27042 son las directrices para el procedimiento de la actuación pericial en el escenario de la identificación y análisis de la evidencia digital, hasta que ésta se considera apta para ser prueba judicial. .

CASOS INTERNACIONALES CON ERRORES EN EL TRATAMIENTO DE LA EVIDENCIA DIGITAL

Como dije, los operadores concientizados sobre el tratamiento de la evidencia digital, somos testigos de la mala experticia en la materia. A modo de ejemplo basta mencionar el caso Martinelli quien es el expresidente de Panamá, fue acusado de autorizar escuchas ilegales con el programa Pegasus. Lo absolvieron en dos instancias por errores en el tratamiento de la prueba digital, dado que no hubieron registros de cadenas de custodia de la evidencia digital, los correos electrónicos se expusieron como capturas de pantalla o en archivos pdf sin su metadata, otros documentos digitales no fueron hasheados, esto es pesados o medidos digitalmente, ni existieron informes de expertos.

Otro caso que aún se encuentra en trámite es el de André Conte de Panamá, en donde el imputado actualmente esta cumpliendo prisión preventiva morigerada en su domicilio, siendo acusado de un delito contra la seguridad de los medios electrónicos en perjuicio del Estado Panameño, en donde además de violaciones a garantías constitucionales y procedurales, registra una mala manipulación de la evidencia digital.

En primer lugar, la información a la que supuestamente accedió Andre, fue publicada en una página adjudicada a otra persona (anonimus Panamá) y como medida principal la policía requirió al sitio web que la evidencia sea eliminada, con lo cual no hay prueba con que cotejar,

Parte de los secuestros no fueron debidamente documentados, al realizar la extracción de datos de los dispositivos se usaron ordenadores con software vencidos, trabajaron sobre la evidencia original no sobre copias, los investigadores y fiscales manipularon los dispositivos en forma directa ante las partes para luego de ello cedérselos a los peritos informáticos e hicieron múltiples extracciones de un mismo dispositivo en distintos tiempos sin especificar razones de su necesidad.

Finalmente, otro ejemplo de mala manipulación de la evidencia digital es el del especialista en ciberseguridad uruguayo Daniel Alberto Hill, quien fue arrestado y puesto en prisión preventiva como consecuencia de una investigación que roza lo ridículo dado que los investigadores del caso cuando allanaron su casa, con el pretexto de investigar un delito de acceso ilegítimo a un sistema informático de acceso restringido, secuestraron dos monedas que representaban cada uno un bitcoin, y lo hicieron pensando que realmente eran la representación física de las conocidas criptomonedas, dado que hasta las secuestraron judicialmente junto a material que el experto en ciberseguridad usaba para su labor investigativa diaria.

No hay excusas para el tipo de tratamiento que recibe esta evidencia. Básicamente porque la evidencia digital debe estar soportada en el mismo formato, en dígitos no en papel. Todo lo que se ve se puede manipular múltiples formas, algo que ningún notario podría identificar a simple vista.

DE LA VALORACIÓN DE LA EVIDENCIA DIGITAL

Así como los distintos procesos tienen etapas para la introducción y producción de la prueba, hay etapas específicas de valoración de la misma.

Por ejemplo en las etapas iniciales de todo proceso, ni las partes ni el juez ofrecen certeza absoluta sobre las mismas, por lo que practican meras revisiones de los estándares legales de recolección y valoraciones en cuanto a la posibilidad que esos elementos tienen de a partir de su análisis se coliga la verdad de lo ocurrido.
Es que la función de la prueba es justamente la de ofrecer al juez elementos para establecer si un determinado enunciado, relativo a un hecho, es verdadero o falso.

La prueba es un instrumento de conocimiento. La evidencia digital, es un tipo de prueba cientifica, no es similar a una testimonial que es muy subjetiva y de la cual se pueden extraer, erróneamente apreciaciones personales por parte del juez. La evidencia digital aporta datos objetivos al pleito, no tiene puntos de vista. El profesor Taruffo decía que en un cierto sentido, la ciencia y el proceso tienen un objetivo común: la investigación de la verdad y que la investigación científica está de por sí orientada hacia la búsqueda de la verdad como el proceso judicial.

En general a medida que se superan las etapas del proceso las exigencias sobre la valoración de los elementos probatorios se va incrementando.

En la etapa del debate oral, donde se produce la prueba ofrecida en instancias anteriores, el juez está autorizado a efectuar una valoración de las mismas para advertir en qué grado contribuye a construir esa verdad.
.

En los procesos no penales utilizará criterios de probabilidad, la hipótesis más probable o la probabilidad prevalente y, en los procesos punitivos el criterio es la prueba más allá de toda duda razonable.

El criterio de la probabilidad prevalente implica que, entre las diversas hipótesis posibles en torno a un mismo hecho, deba preferirse aquella que cuenta con un grado relativamente más elevado de probabilidad.

El estándar de la prueba más allá de toda duda razonable trata de lograr que el juez penal pueda condenar al imputado solamente cuando haya alcanzado la "certeza" de su culpabilidad. La certeza es un grado mayor al de la probabilidad. La evidencia digital bien manipulada aporta un grado de certeza mayor al de otras pruebas no científicas.

CONCLUSIONES

No se puede hacer justicia a cualquier costo, solo haciendo justicia. En definitiva los operadores del sistema judicial deberán ajustar sus comportamientos a reglas que favorezcan el respeto irrestricto por los derechos y garantías constitucionales, convencionales y procesales de todos los involucrados, tanto victimas como victimarios., sencillamente porque el fin no justifica los medios y la obtención del conocimiento, actualización y capacitación constante de los operadores judiciales es una obligación de los Estados. El tratamiento de la evidencia digital debe ser el adecuado, conforme a las reglas y protocolos preestablecidos y conocidos de antemano, mediante procesos verificados que sean factible de ser cotejados en instancias posteriores.

BIBLIOGRAFIA CONSULTADA

1 Norma ISO/IEC 27037:2012; 2 Norma ISO/IEC 27042:2015, RCC 3227

2 https://www.dw.com/es/absuelven-a-expresidente-martinelli-por-caso-de-escuchas-ilegales/a-59772948 consultado el 15/11/2021

4 https://www.youtube.com/watch?v=DMMCx6D7v0M consultado el 10/11/2021

5 THE BEST PRACTICES FOR SEIZING ELECTRONIC EVIDENCE, VERSIÓN 3.0, US. Department of Home Land Security, and the United States Secret Service

6 Téllez Valdez, Julio: “Derecho Informático” 3era ed. Ed. Mc Graw Hill Mexico. 2003.

7 SANTIAGO ACURIO DEL PINO Profesor de Derecho Informático de la PUCE Delitos Informáticos: https://www.oas.org/juridico/spanish/cyb_ecu_delitos_inform.pdf consultada el 13/11/2021

8 Gercke, Marco. Informe “Comprensión del ciberdelito: fenómenos, dificultades y respuesta jurídica". Esta publicación está disponible en línea en: www.itu.int/ITU-D/cyb/cybersecurity/legislation.html impreso en Suiza Ginebra, 2014.

9 TARUFFO, MICHELE, La Prueba. Artículos y conferencias (2009) Editorial Metropolitana.

Autora: Mariel Suárez. Jueza Penal (Chubut) Argentina. Experta en Derechos Digitales, Cibercrimen, Ciberseguridad y Extracciones forenses. Docente Universitaria. Autora de publicaciones varias. Ponente internacional.

La prospectiva: El arte de prever el futuro

Resumen: La prospectiva es una técnica que se viene utilizando en muchos de los campos en los que se manejan escenarios e hipótesis futuras, basados en la estrategia y en el análisis de las variables. Los Analistas de Inteligencia, a menudo, se encargan de proyectar dicha técnica, debiendo manejar otros muchos procedimientos analíticos y exponiéndose a tesituras que no siempre son imaginables en la actualidad o en tiempos pasados; véase el caso de los talibanes en Afganistán, o del COVID-19 en todo el mundo.

Saber emplear la prospectiva con rigurosidad, hará que organizaciones y Estados puedan prever el futuro, establecer su presente y ser más competitivos en términos geoestratégicos y geopolíticos.

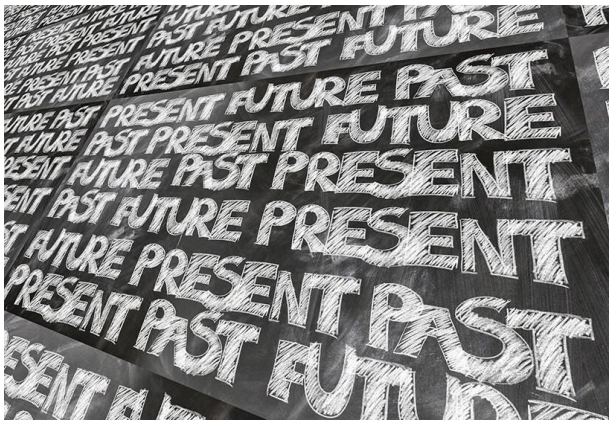
Palabras clave: Prospectiva, inteligencia, geoestrategia, geopolítica, análisis.

DESARROLLO

La RAE define la prospectiva como el "conjunto de análisis y estudios realizados con el fin de explorar o de predecir el futuro en una determinada materia". El Instituto de Prospectiva Estratégica de España (1999), enmarca a la prospectiva como "una disciplina con visión global, sistémica, dinámica y abierta que explica los posibles uturos, no sólo por los datos del pasado, sino

fundamentalmente, teniendo en cuenta las evoluciones futuras de las variables -cuantitativas y cualitativas-, así como los comportamientos de los actores implicados, de manera que reduce la incertidumbre, ilumina la acción presente y aporta mecanismos que conducen al futuro aceptable, conveniente o deseado".

En este sentido, la prospectiva se utiliza dentro del Análisis de Inteligencia para prever escenarios futuros a partir de una serie de análisis de posibilidades, en función de una información obtenida, todo ello pasando por un proceso de revisión constante y encontrándose sujeto a modificaciones. Por ejemplo, hace unos pocos días, EEUU vaticinaba que los talibanes tardarían un largo tiempo en tomar Afganistán. Posteriormente, ese tiempo se redujo a una semana, y fue tan sólo unos pocos días los que necesitaron, finalmente, los talibanes para tomar todo el territorio afgano.



Estas declaraciones no se encuentran basadas en la presuposición o el azar, sino que tendrán su razón teniendo en cuenta que una de las técnicas que se pueden emplear para el desarrollo de análisis prospectivos es el de la monitorización mediante OSINT y SOCMINT de personajes clave dentro del mundo talibán, conociendo sus lazos más estrechos y

sus futuros movimientos. Aun así, esto no siempre es suficiente, y se demuestra que la realidad avanza muy deprisa y que los procesos de revisión y modificación deben ser constantes.

Por otro lado, y en términos de geoestrategia y geopolítica, el Coronel Pedro Baños escribe en su libro 'Así se domina el mundo' que la geopolítica actual ya no debe considerarse solamente como la influencia que se determina dentro de un único territorio o zona, sino más bien, como la acepción que vincula el poder de un estado a escala internacional, la posibilidad de dominar los porvenires del planeta sin que otros estados puedan influir sobre ellos; es decir, la geopolítica de un país va a necesitar regirse por un ejercicio de prospectiva; unas directrices diseñadas en la actualidad, que le permitan establecer el rumbo para alcanzar unos objetivos futuros.

En este sentido, el Consejo Nacional de Inteligencia de los Estados Unidos desarrolla unos informes quinquenales llamados 'Global Trends'. Estos informes suponen un análisis prospectivo de diferentes aspectos relacionados con la sociedad, las políticas, las relaciones entre Estados, el medio ambiente, la tecnología o el desarrollo humano. En ellos se evalúan las tendencias e incertidumbres claves a la hora de desarrollar una estrategia de Estado y que, sin olvidar que se trata de la mayor potencia mundial, deben ser entendidos más bien como una forma de modelar el mundo, que como una pura predicción.

En entornos de alta incertidumbre, con cambios veloces y de gran complejidad como los que se desarrollan en las sociedades occidentales hoy en día, y por ende, en el marco de la geopolítica mundial, los modelos predictivos deben tratar de ofrecer escenarios de futuro, para adoptar en el presente las medidas que nos llevan al futuro deseado, o al menos eviten los indeseados. Es ahí, donde la definición que Gaston Berger daba sobre la prospectiva en 1991, cobra sentido, al decir que "se trata de una ciencia que estudia el futuro para comprenderlo y poder influir en él", adquiriendo, por tanto, un carácter fundamentalmente estratégico.

Con todo ello, y enmarcando la prospectiva en un contexto histórico actual, no va a resultar sencillo el uso de esta técnica, pues hoy en día se manejan cantidades ingentes de información, se tiende al cortoplacismo y la urgencia, se superponen los localismos y nacionalismos frente a los globalismos y, pese a la especialización de los profesionales, no todos los Estados y organizaciones cuentan con los mismos recursos, intereses ni estrategias.

Lo que está claro es que, a la hora de realizar un análisis prospectivo, se debe de esclarecer, primeramente, el objeto de estudio a tratar, el marco temporal y geográfico sobre el cual lo queremos delimitar y el fin que se va a buscar a través de dicho análisis. No se debería olvidar que este estudio va a poder apoyar el diseño estratégico, táctico y operativo de las organizaciones.

Además, este proceso requiere una revisión constante, ya que no siempre se habrán utilizado las técnicas más adecuadas, no se habrán considerado los elementos más óptimos o podrían aparecer indicadores nuevos, que no se habían considerado y que pueden tener especial influencia en los

escenarios futuros. Por ejemplo, se habían realizado análisis prospectivos teniendo en cuenta la posibilidad de una pandemia a nivel mundial, originada por un virus. Sin embargo, cuando apareció el COVID-19, se vio que los posibles escenarios que se habían descrito no alcanzaban la magnitud real de la importancia e influencia que tiene en la actualidad.

El manejo de diferentes técnicas analíticas como el OSINT; el análisis DAFO, que le permita diferenciar los factores que afectan al fenómeno que se está analizando, así como su evaluación e impacto; o el análisis de actores MACTOR, que establece los actores involucrados dentro del estudio analítico, sus objetivos y sus influencias cruzadas; junto a, la ya explicada, constante revisión y actualización e, incluso, la posterior revisión por otro equipo de analistas, va a suponer una notoria mejora del análisis prospectivo realizado y, por tanto, un mejor estudio de los escenarios futuros, en función de la situación actual y del pasado conocido. Asimismo, el hecho de que diferentes grupos de inteligencia adquieran las mismas conclusiones o presupongan los mismos escenarios, por cuenta propia, es una muestra más de que las hipótesis planteadas son posibles y ciertamente realizables.

En definitiva, la prospectiva es una técnica valiosa, útil y recomendable si lo que se desea, como organización o Estado, es establecer un rumbo estratégico, que permita alcanzar unos intereses sociales, políticos, económicos y tecnológicos, con los que poder someter los intereses nacionales a los intereses geoestratégicos y geopolíticos que, como bien ya se ha dicho, serán de carácter global. Gracias a poder prever escenarios futuros y situarse en ellos, se podrá virar a un lado u otro, eligiendo la travesía y, sobre todo, el puerto a alcanzar.

Autor: Mario Bautista Rubiera. Criminólogo y colaborador del Área de Análisis de Inteligencia y Ciberseguridad en Sec2Crime.

Tanatología: Un Antes y un Después

Resumen: La tanatología según la Real Academia Española se define de dos maneras: "el conjunto de conocimientos médicos relativos a la muerte" y desde el punto de vista de la medicina legal, como "el estudio de los efectos que produce la muerte en los cuerpos". (Real Academia Española)

LA TANATOLOGÍA

La tanatología tiene su origen en el griego: Thanatos (muerte) y en logos (estudio); y las principales funciones se centran en preparar y ayudar a pacientes terminales y a sus familiares, así como dar a conocer el principio de autonomía, que se entiende como aquel que permite al individuo tomar las decisiones relacionadas con el proceso de la muerte.

Dentro del proceso de la muerte podemos encontrar 3 tipos: la eutanasia, la ortotanasia y la distanasia. La eutanasia está compuesta por las palabras eu (bueno) y thanatos (muerte) y se entiende como aquella conducta intencionalmente encaminada a finalizar la vida de una persona que padece una enfermedad grave e irreversible, por razones médicas o por compasión.

Por otro lado, se encuentra la ortotanasia compuesta por orthos (recto/ajustado) y thanatos , esta se define como aquel proceso que ayuda al paciente a morir en su debido momento. Es por eso que este recibe los cuidados y tratamientos necesarios con lo que disminuir el sufrimiento, pero sin trastornar el curso de la enfermedad que padece y por tanto el curso de la muerte.

Por último, se encuentra la distanasia, compuesta por las palabras dis (mal) y thanatos (muerte), y se entiende como aquella prolongación innecesaria del sufrimiento de un paciente terminal , a través de medicación o acciones que le "mantienen o le calman", prolongando así su vida de manera innecesaria, sin tener en cuenta la calidad de vida del enfermo.

Los signos de muerte se dividen en dos grupos: los signos clínicos como pueden ser la suspensión de la actividad cardiovascular, la suspensión de la actividad nerviosa y la suspensión de la actividad respiratoria. Y los signos de carácter biológico, como pueden ser la hipotermia, rigidez, livideces y la descomposición orgánica.

SIGNOS Y TIPOS DE MUERTE

En cuanto a los tipos de muerte, existen hasta 6 tipos: la muerte biológica o real, aquella que se da por la ausencia de actividad vital. La muerte aparente se da con la atenuación de las funciones vitales como puede ser un coma, un sincope, etc.

La muerte relativa es por otro lado la suspensión efectiva de las funciones tanto cardiocirculatorias, como respiratorias y neurológicas, pero con la posibilidad de reanimación del individuo.

La muerte súbita ocurre de forma inesperada y no violenta en individuos que no tienen por qué padecer una enfermedad frente a la muerte repentina, que ocurre de forma rápidaen individuos que si que sufren una enfermedad. Por ultimo la muerte natural, aquella producida por cualquier patología o enfermedad.

FENÓMENOS CADAVÉRICOS

Los fenómenos cadavéricos tardíos se dividen en Autolisis y putrefacción.
La primera se define como el conjunto de procesos fermentativos anaeróbicos que ocurren en el interior de la célula por acción de las enzimas celulares, sin acción bacteriana, mientras que la putrefacción se define como la fermentación pútrida de origen bacteriano
que tiene origen en la zona externa como pueden ser los órganos respiratorios o en la zona interna como puede ser el intestino.

El proceso de putrefacción transcurre por distintas fases; la fase cromática, que se inicia con una mancha verde en la fosa iliaca derecha transcurridas 24-36h hasta que se transforma en una mancha pardonegruzca y su duración es de días. Después se encuentra la fase enfisematosa, se producen gases y el cadáver se hincha, suele ocurrir a las 48h del fallecimiento y dura unas 2 semanas. A continuación, se produce la licuefacción, el tejido blando se licua, se reblandecen los órganos (próstata y útero resisten más), se produce la perdida de gases y tiene una duración de entre 8 y 10 meses.

La última fase, también llamado reducción esquelética se caracteriza por la desaparición de las partes blandas y tiene una duración de entre 2 y 5 años, y unos 50 años para que suceda la pulverización.

El proceso de la putrefacción se puede ver afectado por distintos fenómenos, éstos pueden ser individuales (constitución física y edad), patológicos (putrefacción rápida y putrefacción lenta), o ambientales (humedad, frio, aire, etc) sin embargo existen fenómenos que por el contrario conservan el cadáver. [2]

.

Estos fenómenos conservadores son, la momificación; este proceso produce la deshidratación de los tejidos y dura entre 1 y 12 meses (las zonas con climas secos, cálidos y con corrientes de aire favorecen este proceso). Otro fenómeno conservador es la saponificación; este proceso consiste en un cambio químico de las grasas corporales que acaban convertidas en “jabón”; suele ocurrir en cadáveres que han estado sumergidos en agua y dura entre 3 y 12 meses. Otro método de conservación es la corificación, el cuerpo pasa a un estado en el cual la piel se asemeja al cuero, con un color gris amarillento y de consistencia blanda. Para ello es necesario incorporar al cadáver en una caja de zinc soldada; este proceso dura entre 1 y 2 años.

Por último, tenemos el proceso de la congelación; para ello es necesario que el cadáver se encuentre en un entorno con temperaturas de entre 0 y grados centígrados.

ENTOMOLOGIA CADAVÉRICA

La entomología cadavérica o forense se define como “el estudio de los insectos, de sus larvas y de las crisálidas que se encuentran en el cadáver.

Su interés desde el punto de vista de la medicina legal radica en que permiten determinar de forma bastante aproximada la fecha de la muerte, teniendo en cuenta las especies encontradas y su grado de evolución en relación con la época del año y las condiciones ambientales”. (clínica Universidad de Navarra)

Se estudia el Cuándo, el Cómo, y el Dónde. Dentro de las familias de insectos, cabe destacar a los dípteros o moscas que son los primeros en llegar al cadáver. Si se conoce el ciclo de vida de este grupo de insectos se puede determinar la edad del animal, la cual es proporcional a la data de la muerte.

OPERACIONES TANATOLÓGICAS

Las operaciones tanatológicas son un conjunto de procesos que se dividen en el levantamiento del cadáver, el examen externo y el examen interno:

LEVANTAMIENTO DEL CADÁVER

El levantamiento del cadáver se entiende por la diligencia judicial que tiene por objeto examinar el cadáver en el lugar de los hechos; ésta debe contar siempre con un médico forense. Existen fases para llevar a cabo dicho levantamiento: primero debe de protegerse el lugar de los hechos, se debe de observar el lugar y delimitarlo. Una vez delimitada la escena, se realiza una descripción del cadáver in situ y se procede a su traslado al respectivo anatómico forense. [3]

En este procedimiento participan la Comisión judicial, tanto juez instructor como el secretario, el perito forense y la policía judicial, toso ellos con el objetivo de precisar y evaluar las circunstancias en que se encontró el cadáver, para su posterior traslado al Instituto de Medicina Legal donde se realizaran los estudios forenses y la investigación policial.

EXAMEN EXTERNO DEL CADÁVER

Este proceso se centra en la inspección detallada del cadáver antes de proceder al examen interno. Dicho inspección debe centrarse en los signos relativos a la identificación del cadáver (edad, talla, sexo, ropa, objetos personales, color de pelo…), en los signos relativos a la data de la muerte (enfriamiento, rigidez, deshidratación, livideces, putrefacción), además de en los signos relativos a la causa de la muerte (lesiones traumáticas, desnutrición…), también en los signos relativos al medio donde estaba el cadáver (momificación, saponificación…) y por último en los signos relativos a las circunstancias de los hechos (estado de orificios corporales (ano, boca…), señales de inmovilización, arrancamiento…).[4]

EXAMEN INTERNO DEL CADÁVER

El examen interno del cadáver constituye el último proceso dentro de las operaciones tanatológicas. Consiste en la apertura del cadáver y debe hacerse en el siguiente orden:

- 1. Columna vertebral (ocasionalmente)
- 2. Cráneo
- 3. Cuello
- 4. Tórax
- 5. Abdomen
- 6. Aparato genitourinario
- 7. Extremidades

Autora: Gema Simón Alberola. Estudiante de Criminología y colaboradora del Área de Criminología en Sec2crime.

EVENTOS

Como parte de su dimensión divulgativa/*think tank,* Sec2crime organiza eventos como conferencias, paneles, mesas redondas y debates con el objetivo de concienciar a la sociedad en materia de Seguridad, Criminología, Delincuencia Económica, Prevención del Terrorismo, Conflictos Armados, Análisis de Inteligencia, Ciberseguridad y Defensa.

Octubre 2021
Mesa Redonda “Jóvenes y cultura de Defensa”.

Septiembre 2021
Seminario “Criminología en prisiones“.

Julio 2021
Presentación del documento “Tendencias online de la propaganda yihadista. Análisis del caso español”.

Mayo 2021
Jornada de presentación del Comité de Expertos de Sec2crime.

Abril 2021
I Jornadas Sec2crime.

Marzo 2021
Agenda 2021: mujeres y retos futuros.

Febrero 2021
Evento: ¿Criminología y prisión?

SEC2CRIME
FROM SECURITY TO CRIME PREVENTION

COMITÉ DE EXPERTOS

A continuación les presentamos una serie de entrevistas realizadas a los y las profesionales que integran nuestro Comité de Expertos, con el fin de poder completar esta memoria de Sec2Crime 2020-2021 y poner en valor su trayectoria y experiencia en distintos campos vinculados a la seguridad. Siempre es un placer contar con su participación en las distintas actividades que venimos desarrollando.

Sec2Crime ha constituido, recientemente, un Comité de Expertos, formado por perfiles de reconocida experiencia:

Eugenia Hernández, Directora de UNINT (Unidad de Análisis de Inteligencia de la Universidad Autónoma de Madrid) y diplomada en Altos Estudios de Defensa Nacional (CESEDEN).

Eugenia Hernández

Matteo Re, Doctor en Historia Contemporánea, investigador y Profesor en el Máster "Análisis y prevención del terrorismo" de la Universidad Rey Juan Carlos.

Matteo Re

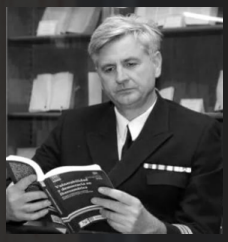
Paz Velasco de la Fuente, Criminóloga y jurista especializada en personalidad psicopática y delitos violentos. Escritora y creadora de "Criminal-mente".

Paz Velasco de la Fuente

Edo Bakker, CEO de Agile Control Solutions. Asesor y Experto Externo registrado en Prevención del Blanqueo de Capitales y Compliance.

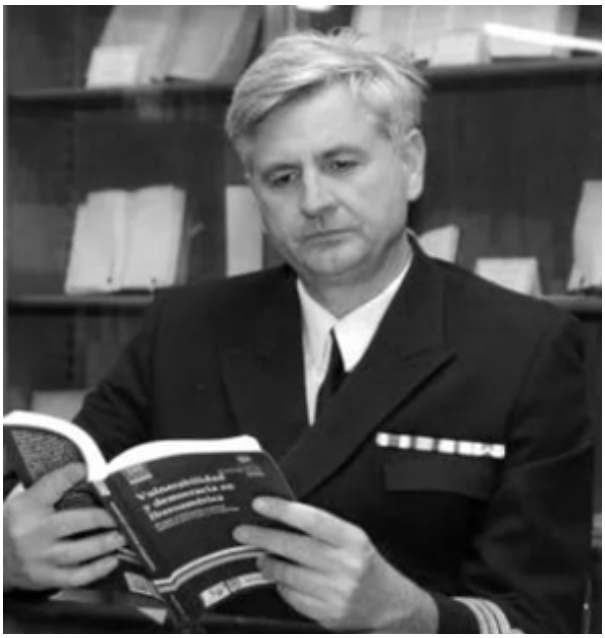
Edo Bakker

Federico Aznar Fernández Montesinos, Doctor en Ciencia Política, escritor, militar, ensayista y profesor universitario.



Federico Aznar Fdéz-Montesinos

Federico Aznar Fdez- Montesinos



Doctor en Ciencia Política, escritor, militar, ensayista y profesor universitario.

¿QUÉ VALOR CREE QUE APORTA O PUEDE APORTAR SEC2CRIME AL SECTOR DE LA SEGURIDAD?

Ofrecer un espacio de reflexión académica en que sus miembros también se den a conocer mientras dan cuenta de la calidad de su trabajo. Es un foro atípico y por ello de particular interés.

¿CUÁLES CREE QUE SON LOS PRINCIPALES RETOS ACTUALES EN EL ÁREA DE LA PREVENCIÓN DEL TERRORISMO YIHADISTA?

Los lobos solitarios y los problemas de orden público que generan no son de suficiente entidad, esto es, relevantes desde la perspectiva de la Defensa. El riesgo que el terrorismo yihadista plantea es que vuelva a los grandes atentados que son los únicos que le han dado notoriedad y relevancia internacional. Desde el 11-S sólo ha conocido la decadencia; ha perdido la iniciativa y la libertad de acción hasta quedar fuera del espacio mediático.

EN MÚLTIPLES OCASIONES, USTED HA EXPLICADO SUS REFLEXIONES SOBRE EL CONCEPTO DE GUERRA, ¿CUÁL SERÍA LA EVOLUCIÓN Y EL CAMBIO QUE, A SU PARECER, HA ATRAVESADO ESTE TIPO DE CONFLICTO, DESDE LAS GUERRAS DE LOS PRIMEROS AÑOS DEL 2000 A LOS AÑOS ACTUALES?

La guerra no ha cambiado su naturaleza que es política por más que haya cambiado su forma. La tecnología y el desarrollo afectan a la forma en que se hace la guerra, pero no afectan a su esencia. El concepto de zona gris atiende a la complejidad de las Relaciones Internacionales y al incremento de estas. A más relaciones más conflictos, aunque a causa de estas, de menor intensidad. Política y conflicto se superponen en un mundo de relaciones híbridas, en las que los países en unas áreas compiten, en otras rivalizan. En este contexto la diversidad de intereses hace muy difícil que puedan darse hoy guerras en un sentido convencional.

Matteo Re

Doctor en Historia Contemporánea, investigador y Profesor en el Máster "Análisis y prevención del terrorismo" de la Universidad Rey Juan Carlos.

¿QUÉ VALOR CREE QUE APORTA O PUEDE APORTAR SEC2CRIME AL SECTOR DE LA SEGURIDAD?

Creo que todo tipo de labor seria y contrastada como es el que realiza Sec2Crime tiene un gran valor en los estudios sobre seguridad. Crear vínculos y una red para facilitar la difusión de contenidos de investigaciones, también en su faceta divulgativa, favorece la accesibilidad a temas de seguridad, a menudo complicados y enrevesados.

¿CUÁLES CREE QUE SON LOS PRINCIPALES RETOS ACTUALES EN EL ÁREA DE PREVENCIÓN DEL TERRORISMO?

En mi opinión hay dos retos muy diferentes entre ellos. El primero tiene que ver con una labor de prevención de la radicalización entre los jóvenes admiradores de la izquierda abertzale que, al no haber vivido los años de ETA, miran hacia ese periodo con una cierta ignorante admiración. Por otra parte, y este sería el segundo reto -uno de los temas más candentes en la actualidad- hace falta llegar a un acuerdo a nivel internacional sobre cómo actuar con los combatientes terroristas extranjeros detenidos en Siria y en Irak. Ese esfuerzo tiene que extenderse también a mujeres y niños del Daesh.

VISTO QUE LA MAYORÍA DE LOS PAÍSES DEL MUNDO ESTÁN BAJO LA LUPA DE GRUPOS TERRORISTAS DE CORTE YIHADISTA, ¿CÓMO DE IMPORTANTE ES LA COLABORACIÓN INTERNACIONAL PARA LA DETECCIÓN Y DETENCIÓN DE DELITOS RELACIONADOS CON EL TERRORISMO?

La colaboración internacional para contrarrestar el terrorismo es fundamental. Lo hemos comprobado tras el 11-S y lo comprobamos a diario no solo con el terrorismo yihadista, sino también con el crimen organizado. Las mafias, por ejemplo, solo se pueden contrarrestar gracias a una red de inteligencia a nivel supranacional. Lo mismo, como es obvio, ocurre con el terrorismo, el cual, al haberse globalizado, no entiende de fronteras ni físicas ni ciberespaciales. Es allí donde la colaboración entre Estados y entre Policías de diferentes países resulta ser crucial para contrarrestar este peligro constante.

Edo Bakker

CEO de Agile Control Solutions. Asesor y Experto Externo registrado en Prevención del Blanqueo de Capitales y Compliance.

¿QUÉ VALOR CREE QUE APORTA O PUEDE APORTAR SEC2CRIME AL SECTOR DE LA SEGURIDAD?

Sec2Crime aporta mayor visibilidad al sector de la Seguridad para el público general. La mayoría de la gente desconoce la amplitud del sector y muchas veces solo se asocia Seguridad con la seguridad física o vigilantes de seguridad. En realidad el sector abarca campos como la criminología, criminalística, ciberseguridad, análisis de inteligencia, delincuencia económica, seguridad física etc.

¿CUÁLES CREE QUE SON LOS PRINCIPALES RETOS ACTUALES EN EL ÁREA DE LA SEGURIDAD EMPRESARIAL Y FINANCIERA?

Pienso que los principales retos están relacionados con cómo sacar más información de valor de la cada vez más mayor disponibilidad de información sin morir en el intento. Por otro lado, en áreas como la prevención del blanqueo de capitales y el Compliance en general todavía muchas empresas están en un nivel de cumplimiento bastante bajo. Esto puede ser una amenaza en un mundo donde las autoridades cada vez disponen de más información y también porque muchas veces no se conoce con quienes se establecen relaciones de negocios (clientes, proveedores, distribuidores, empleados etc).

EN ESPAÑA NO EXISTE REGULACIÓN NI NORMATIVA RESPECTO A LAS CRIPTOMONEDAS, ¿ESTO LE PARECE QUE AÑADE PELIGRO A LA MANIPULACIÓN Y USO DE ESTA "DIVISA"?

Claramente conlleva riesgos como el abuso de mercados, fraude, el blanqueo de capitales y la financiación del terrorismo. Recientemente (finales de octubre de 2021) en España se ha avanzado mucho permitiendo a los proveedores de servicios relacionados con criptomonedas el registro en el Banco de España. En este sentido se consolidará más este "nuevo" sector ya que habrá más supervisión, confianza y seguridad jurídica. Las empresas del sector que todavía no habían invertido en cumplimiento normativo lo están haciendo ahora y se están poniendo al día relativamente rápido.

Sec2Crime®
Diciembre de 2021
Madrid - España
https://www.sec2crime.com

SEC2CRIME
FROM SECURITY TO CRIME PREVENTION