AL-GHURABÁ

REVISTA DE CONTRA-NARRATIVA PARA LA PREVENCIÓN DE LA RADICALIZACIÓN VIOLENTA DE ETIOLOGÍA YIHADISTA

FREE COUNTER-NARRATIVE MAGAZINE FOR THE PREVENTION OF VIOLENT EXTREMISM OF JIHADISM ETIOLOGY

by

CISEG

ASPECTOS PSICOSOCIALES

Subyacientes a la radicalización yihadista extrema

DE LAS PANTALLAS A LA REALIDAD

Captación yihadista a través de videojuegos

PALABRAS SECUESTRADAS

YIHAD

ISSUE 47 AGOSTO 2021 ISSN 2565-2222

AL-GHURABÁ

NÚMERO 47 / AGOSTO 2021 / ISSN 2565-2222

Producción y edición
CISEG

Creadores
David Garriga
Marc Fornós

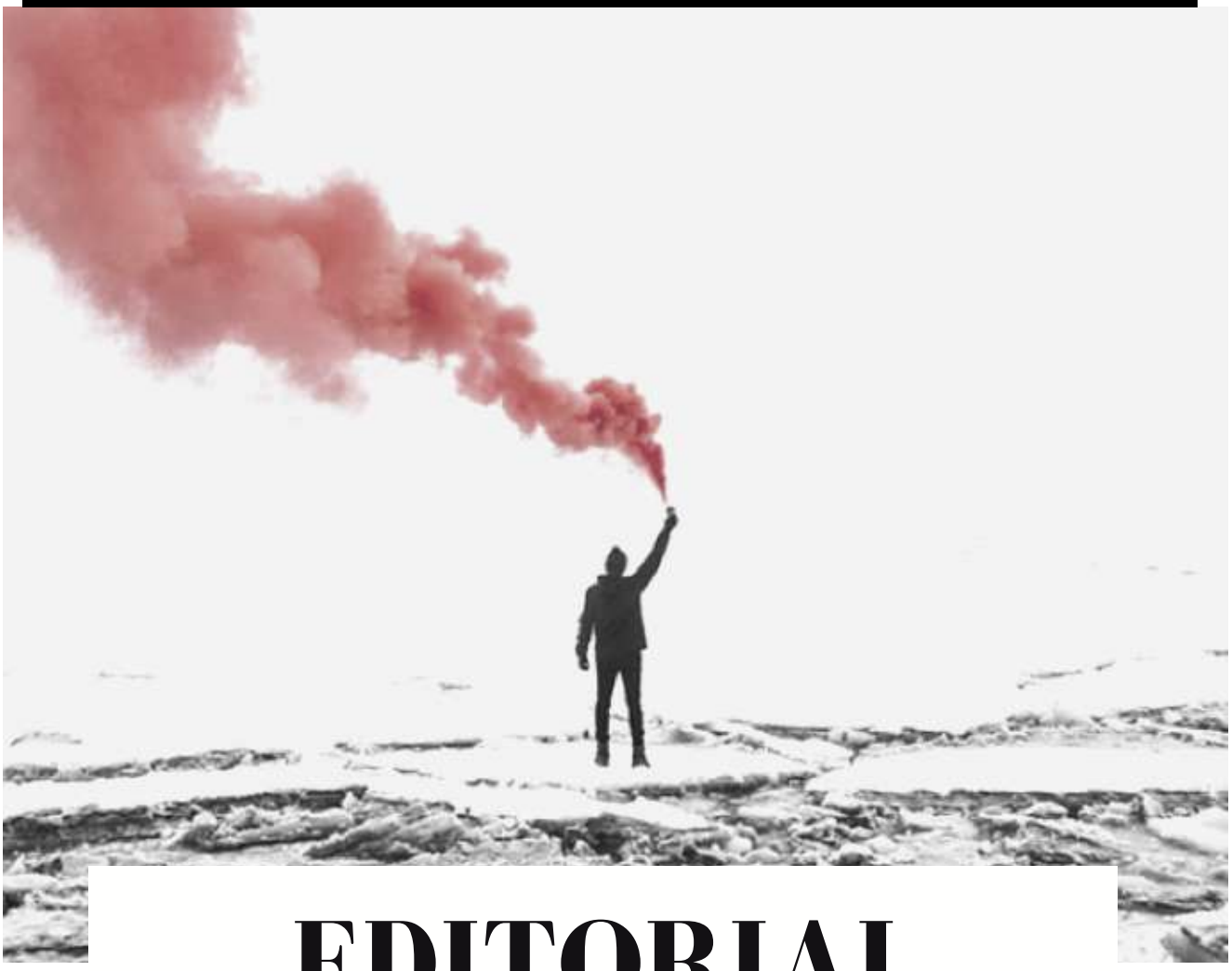
Equipo Redacción
David Garriga
Ariadna Trespaderne

Diseño y Maquetación
Ariadna Trespaderne

CISEG
info@intelciseg.com

Web
www.alghuraba.org

Envío de artículos
alghuraba@intelciseg.com



EDITORIAL

La revista Al-Ghurabá de CISEG, es una herramienta de narrativas alternativas para prevenir la radicalización violenta de etiología yihadista y nace en agosto de 2017 como un proyecto de la Comunidad de Inteligencia y Seguridad Global. Al-Ghurabá es gratuita, on-line y mensual y persigue implicar a la sociedad civil en este sector y ofrecer herramientas de prevención y de contra-narrativa para prevenir la radicalización violenta en el seno de las comunidades a través de publicaciones accesibles realizadas por analistas.

Esta problemática nace en las comunidades, entre las personas y cualquiera puede hallarse en una situación de cercanía con un perfil radicalizado o un agente radicalizador. En consecuencia, brindar herramientas a la sociedad civil permite que sean personas empoderadas, informadas y formadas. Por otro lado, también sirve para difundir contra-narrativa frente a esta radicalización destinada a los grupos más vulnerables a ser radicalizados. El objetivo es crear contenido que analice la situación actual y consiga erosionar y deslegitimar los discursos que facilitan estas organizaciones terroristas.

SUMARIO

IN MEMORIAM

17A

El recuerdo es el diario que todos cargamos con nosotros.

Oscar Wilde

SENTENCIA 17-A

Accede a la sentencia haciendo clic aquí

La Audiencia Nacional condenó el pasado jueves 27 de mayo de 2021 a tres de los acusados de formar parte de la célula terrorista de Ripoll que perpetró los atentados de Barcelona y Cambrils el 17 de agosto de 2017. El atentado dejó 16 muertos y cientos de heridos. Los condenados: Mohamed Houli (53 años y medio de cárcel), Driss Oukabir (46 años de cárcel) ambos por delitos de pertenencia a organización terrorista, fabricación de explosivos y estragos de carácter terrorista. Said Ben Iazza (8 años de cárcel) por colaboración con grupo terrorista. Ninguno de los autores materiales del atentado se pudo llevar a juicio por ser abatidos por la policía. Las víctimas, un total de 16 fallecidos, al menos 200 heridos y otros afectados por estrés post-traumático, según varias asociaciones de víctimas y organizaciones privadas, fueron las más olvidadas.

CUANDO EL CAOS APARECE

José Luis Franco Eza.

Director de Seguridad Privada

José Luis Franco Eza recibió una placa honoraria por la actuación en ese fatídico 17-A durante la XV edición del Día de la Seguridad Privada 2018 en Barcelona.

Poco o nada podía imaginar que aquel 17 de agosto de 2017, se iba a materializar un atentado terrorista como el visto en Niza (Francia) en Barcelona. Los que nos dedicamos a la seguridad, tanto privada como pública, sabíamos que era una amenaza que podía materializarse en cualquier momento, como práctica del "modus operandis" de los grupos de etiología yihadista, pero no lo visualizas en tu ciudad.

Como director de seguridad debes preparar los análisis de riesgos y evaluaciones de estos, con la posibilidad de ocurrencia en tu activo, e idear el plan de autoprotección con los recursos técnicos y humanos necesarios para actuar en primera instancia hasta la llegada de los refuerzos públicos.

En este caso la posibilidad de un IVIMV(Incidente Violento Intencionado con Múltiples Víctimas) es un campo de trabajo que se debe desarrollar y entrenar en los simulacros obligatorios, desde el punto de vista terrorista y social (Persona violenta o AMOK). Estudias los casos ocurridos, tomas apuntes de que se hizo, como se hizo y que salió mal y bien. Estudias tu activo y ves como encajar todas las variables que pueden ocurrir en este tipo de ataques. Casos teníamos de sobras, desafortunadamente. Desde el 2010, las organizaciones terroristas de etiología yihadista han enviado mensajes en sus canales habituales a sus adeptos para usar vehículos como armas y golpear en lugares céntricos, concurridos y en fechas señaladas.

El mercadillo navideño de Berlín en 2016, Niza en pleno 14 de julio, fiesta nacional en Francia, Westminster el 22 de marzo de 2017, Estocolmo el 7 de abril y el puente de Londres, en junio de 2017 donde perdió la vida Ignacio Echeverria, hacían presagiar que podía ocurrir un atentado similar en cualquier región de nuestro país.

Ese día cuando después del trabajo, oyes en las noticias lo que está ocurriendo, sabes que tu sitio no está en casa o lejos del horror, sino que debes dirigirte a él y poner en práctica todo lo que has estado diseñando, estudiando y plasmándolo en protocolos de actuación. Hoy es el día, que sabías que podía llegar.

Llegas a la zona y comienzas a ver el caos que reina en las calles, el despliegue de las Fuerzas y Cuerpos de Seguridad y como las emisoras radian nervios y ordenes que cuesta de entender y menos de cumplir para los que están en primera línea y saben que el autor de la masacre aún puede estar entre esos ciudadanos que corren asustados hacía alguna parte.
Tras solicitar colaboración para entrar en el perímetro e identificarte como Director de Seguridad, obtienes la autorización para entrar y dirigirte a tu activo. Un coche de la Guardia Urbana te traslada hacía él, prestándote esa colaboración que emana de la unión de esfuerzos entre la Seguridad Pública y la Privada.

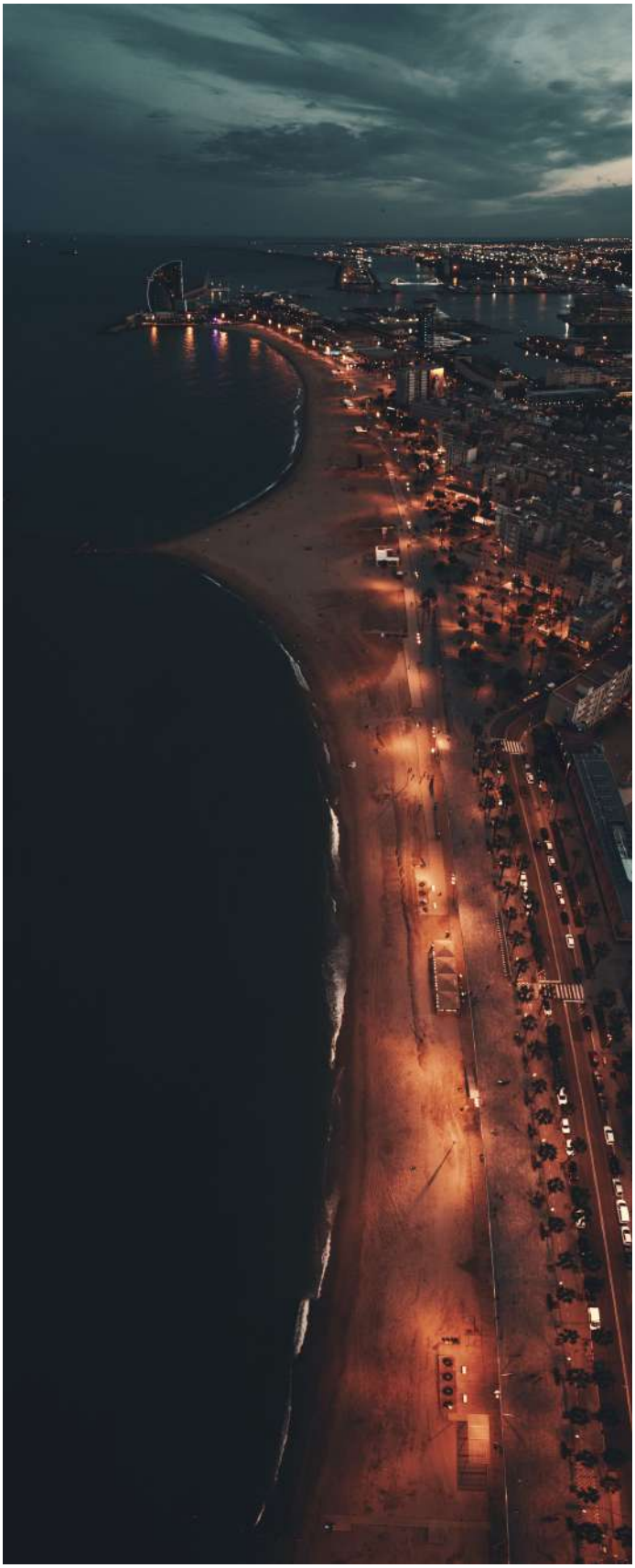
Al llegar aún no eres consciente de que esto es real. Pones a trabajar a tu personal, los vigilantes de seguridad, para prestar la protección que los ciudadanos que se encuentran en el activo buscan. Muchos de ellos se han metido dentro al oír gritos en la calle y gente correr, no saben aún lo que ocurre, algunos hablan de atentado con explosivos, otros tiros y los que han presenciado lo ocurrido ya apuntan a una furgoneta que se ha subido a la acera en las Ramblas de Barcelona.

Ordenas que se cierren las puertas una vez has prestado todo el auxilio necesario. Debes agrupar a las personas en el lugar del activo amplio donde puedas controlarlas mejor, se les hace recoger sus pertenencias, bajo la atenta mirada de los vigilantes de seguridad los cuales están pendientes de movimientos extraños que pueda realizar. Todo lo que haya en suelo, bancos y cualquier lugar debe quedar recogido por alguien que lo identifica como suyo. Se les identifica y comprueba sus pertenencias. Inmediatamente después se realiza una requisa por todos los lugares públicos comprobando que no quede nadie, ni nada sospechoso que pudiese ser un posible artefacto explosivo secundario a la acción principal cometida.

Mientras en la calle, se observa policía de unidades especializadas que empiezan a tomar posiciones e intentan poner luz en el caos existente. Hacen un trabajo excepcional aplicando los protocolos propios de una acción de esta índole que habrán entrenado en previsión de que ocurra. Puedo comprobar como hay policías que han dejado sus familias, amigos o actividades estivales y se han incorporado a Plaza Cataluña con la uniformidad que en aquel momento llevan, haciendo gala de un compañerismo y profesionalidad que se requiere allí.

No es menos el personal de seguridad que atiende en todo momento a las personas confinadas en el edificio. Hay una mujer rusa que muestra el teléfono con la ubicación de su hijo en otro activo cercano al nuestro. Algunos tienen familiares por fuera. Poco a poco van contactando con ellos y transmitiéndose mutuamente tranquilidad. El teléfono es un gran aliado para controlar la escena, pero un altavoz perturbador.

La comunicación entre el exterior e interior se hace a través del teléfono móvil de un mando policial, que de forma muy rápida accede a darme. De esta forma somos conocedores de que es lo que realmente ocurre, ya que las noticias y los WhatsApp que llegan carecen de rigor y muchos de ellos son “fake news” constantes. Esta información se va transmitiendo al público confinado en el interior creando confianza y siendo el único canal de información creíble para ellos. Según pasa el tiempo, cada vez más perciben que están



seguros en el interior.

Mientras, en el exterior continua la policía identificando clientes de bares, a los que sacan en hilera con las manos en la cabeza, como marca el procedimiento policial en estos casos, ya que no se sabía si el autor o autores podían estar ahí. Ambulancias van y vienen en un carrusel constante de ayuda a los heridos, los profesionales sanitarios lo dan todo y su carisma, ternura y rabia por lo ocurrido, se muestra en cada movimiento sobre el herido.

El siguiente movimiento del plan establecido, una vez asegurado el activo e identificado el público que teníamos confinado, es establecer cuando se puede evacuar a estas personas a lugar seguro en el exterior.

El Centro de Control del activo, está en ebullición con llamadas y mensajes de emisora. Ordenar las comunicaciones, las novedades y el silencio radio en estos casos en vital para poder dirigir un equipo en situaciones adversas. Las cámaras controlan el perímetro exterior y las alarmas están en reposo, cualquier salto de alarma nos hará actuar de forma diligente, ya que la amenaza viene del exterior hacía dentro. Por fortuna no ocurre.

Pasadas dos horas y media, se establece la evacuación al exterior del público, fuera del perímetro policial, usando una vía de emergencia subterránea. Se coordina con el operativo policial el movimiento de tal forma que nos esperan a la salida. Un vigilante en punta y otro a cola van sacando grupos de diez en diez, con el fin de que puedan controlarlos con facilidad. Aún no se sabía donde estaba el responsable/s de tal atrocidad.

Una vez está cerrado el activo y las personas evacuadas, tomas conciencia de todo en esos cinco minutos de reflexión personal. Esto ha sido un ataque terrorista en nuestra ciudad y todo aquello que has estudiado, preparado y pensado que debías hacer en una situación así, se ha materializado. Pasadas ya cuatro horas del inicio, aún tienes la adrenalina a

a tope y ves que los compañeros del servicio que te han acompañado en esta cruel travesía lo han dado todo, realizando con éxito todas la ordenes que se les ha dado. Están en modo activo aún, pero en sus caras y en la mía se refleja la satisfacción por el deber cumplido y por como han salido las cosas.

Como lección de aquel fatídico día, como director de seguridad de un activo, sacas estas conclusiones:

Las medidas de seguridad serán siempre preventivas, no esperar que sean reactivas. Si lo son el daño ya se habrá materializado. No debemos ser reactivos, ya que tenemos conocimiento y recursos para dotar de protección a nuestras ciudades, activos y personas que viven o circulan por ellos.

La implantación de medidas de protección, surgen del análisis de la posibilidad de ocurrencia de ataques, como los que se producen en Siria, Irak, Afganistán o en nuestra vieja Europa y su evolución con el uso de nuevas tecnologías: ataques con vehículos usados como armas o con artefactos explosivos VBIED (Vehicle-Borne Improvised Explosive Device), Dispositivos Explosivos Improvisados (IED, por sus siglas en inglés), el uso de DRONES con explosivos o la acción de actor solitario armado (armas de fuego o arma blanca), pueden suceder en cualquier momento y en cualquier lugar.

Los Directores de Seguridad en el ámbito privado, deben ser conscientes de que el terrorismo de etiología yihadista, lamentablemente, estará durante tiempo conviviendo con nosotros. Conocerlo, saber cómo actúa e idear los planes de actuación para hacerle frente es deber profesional. Sabemos la desventaja con la que partimos, ya que el actor solitario o célula terrorista, sabe la respuesta a estas cuatro cuestiones: cuándo, cómo, dónde y por dónde.

La función de los servicios de inteligencia para adelantarse a obtener la respuesta a estas cuatro preguntas es clave en cualquier tipo de terrorismo. Pero no todo el peso de la protección debe caer en los servicios secretos o policías. La seguridad privada debe dar un paso al frente en esta cruzada e implantar medidas valientes, tanto activas, pasivas, humanas y procedimentales para hacer frente en primera instancia a una acción de este tipo, como **PRIMER INTERVINIENTE.**

La formación del personal de seguridad privad es clave. Trabaja como entrenas, entrena como trabajas debe ser tónica constante para las empresas de seguridad, clientes y centros de formación. Exigir una formación real, sin miedos ni tapujos a llamar las cosas por su nombre es función del director de seguridad que va a estar al mando funcional de vigilantes de seguridad que serán el primer uniforme al que acudirá el público en anhelo de su protección. Lo pude comprobar aquel 17 de agosto de 2017.

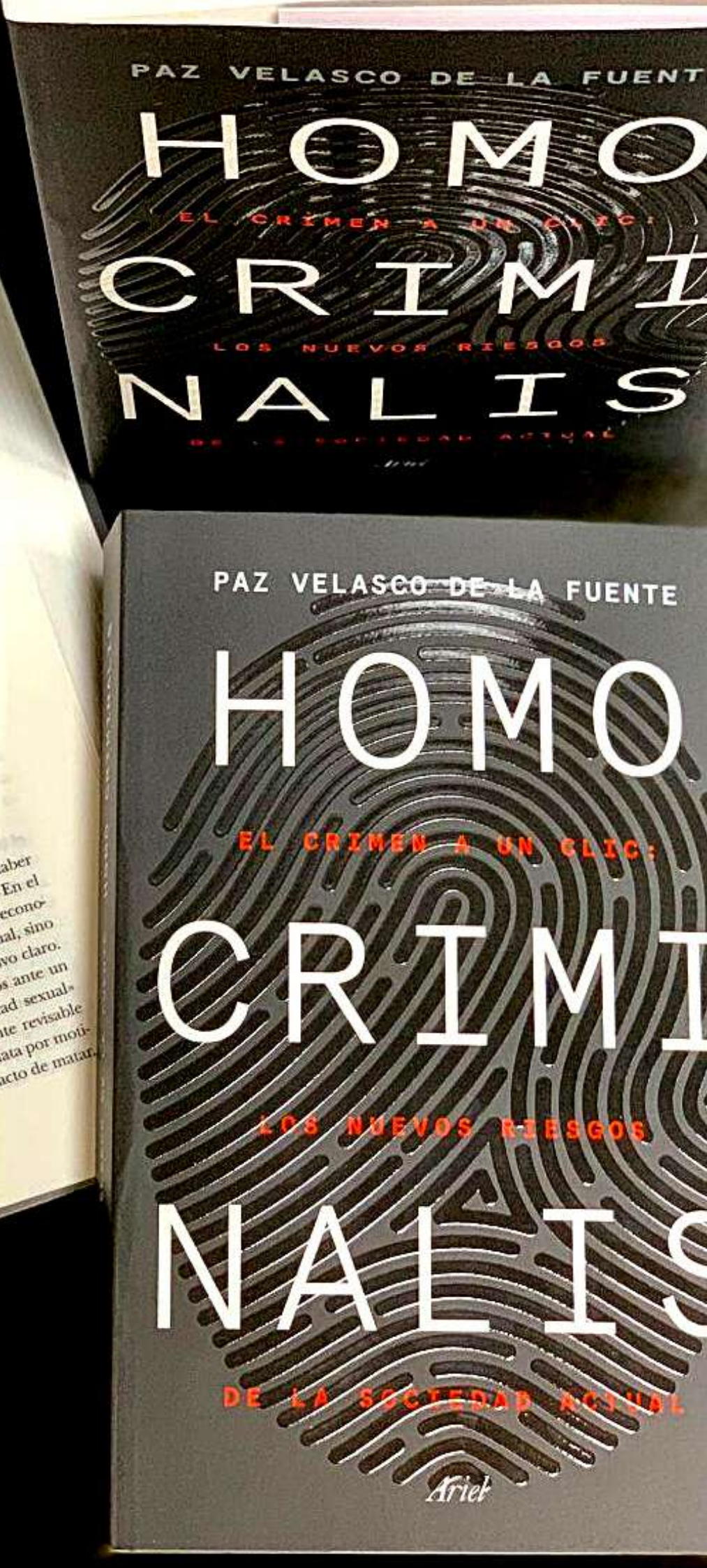
Permítanme dedicar estas letras a las personas fallecidas y heridas, así como a sus familiares. Y desde las mismas, quiero felicitar a todos los profesionales de la seguridad pública y privada que aquel día, dieron un paso al frente cuando todos huían del lugar.

orque su intención es torturar a la
empo posible.
l ascendente según las heridas y las
provocando a la víctima.
excitación sexual, aumenta la agresivi-
en partes del cuerpo con significado se-
genitales, glúteos, boca y ano.
de excitación que les produce torturar a
la agresión es más duradera en el tiempo,
legar a durar horas o incluso días.
estereotipada y ritualista. Infligir dolor a la
s el objetivo de la agresión sexual, no su me-
dental.[20]
encia irá *in crescendo*, lo que puede convertirle en
micida sexual sádico en serie.

motivación sádica, el poder ha de materializar-
través de infligir dolor psicológico y físico a la
ma. El sádico siempre siente placer sexual cuando
ura, sin que sea necesario que se produzca una agre-
n sexual explícita.»[21]

L HOMICIDIO SEXUAL:
EROTOFONOFILIA FRENTE A HOMICIDIO SÁDICO

Debemos diferenciar entre el homicidio cometido tras haber agredido sexualmente a la víctima, y el homicidio sexual. En el primer caso, el agresor mata a su víctima para evitar ser reconocido y denunciado. No estamos ante un homicidio sexual, sino que se trata de un homicidio de utilidad con un objetivo claro. Tras la reforma del Código Penal de 2015, estaríamos ante un asesinato «subsiguiente a un delito contra la libertad sexual» que es castigado con la pena de prisión permanente revisable (art. 140). En cambio, en un homicidio sexual se mata por motivos sexuales, ya que lo que se erotiza es el propio acto de matar.



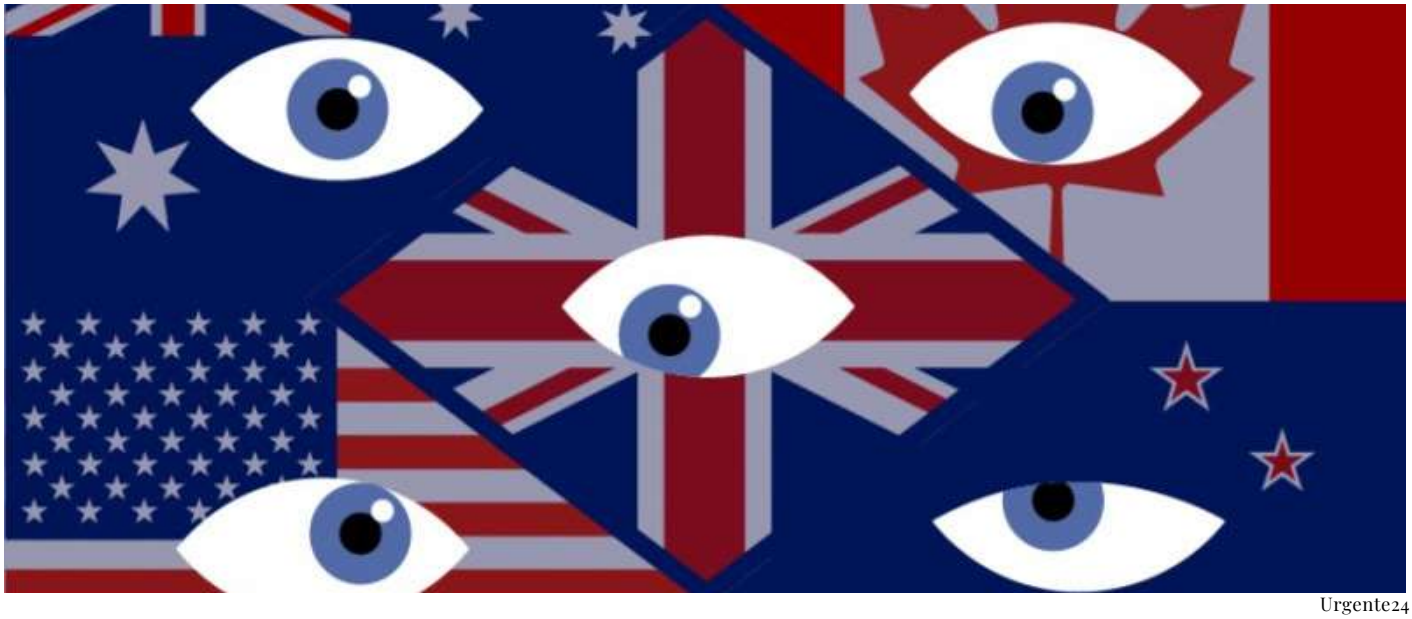
INTELIGENCIA

WWW.ALGHURABA.ORG

LOS FIVE EYES

Y EL MUNDO TRAS LA CRISIS DEL COVID-19

Pablo Andrés Gutiérrez.
Politólogo especializado en las relaciones Unión Europea y Mediterráneo.
Vice Secretario General de European Guanx



Urgente24

Hoy en día, cuando hablamos de los Five Eyes sabemos identificar perfectamente que nos referimos a la alianza entre Estados Unidos, Reino Unido, Canadá, Australia y Nueva Zelanda para compartir toda la inteligencia y la gran mayoría de métodos de obtención de los países involucrados en el acuerdo. Sin embargo, no fue hasta la década de 1990 que esta alianza se dio a conocer al mundo por primera vez y que se hizo más popular tras los documentos filtrados por Snowden.

No obstante, tenemos que remontarnos al final de la Segunda Guerra Mundial para encontrar los pilares fundacionales de esta alianza. En 1941 Winston Churchill y Franklin Roosevelt a bordo de HMS Prince of Wales acordaron compartir la información más delicada que obtuviesen de sus dos grandes enemigos, la Alemania Nazi y Japón, teniendo como principal fuente obtención de información la intercepción de comunicaciones. Tras el final de la guerra y debido al buen resultado que había dado esta cooperación y el desarrollo de las operaciones SIGINT, poniendo como ejemplo la desencriptación de los cables diplomáticos alemanes y japones, Reino Unido y Estados Unidos decidieron continuar y ampliar con su colaboración en inteligencia firmando en 1946 el acuerdo UKUSA antes conocido como BRUSA.

Este tratado bilateral, de solo siete hojas de longitud, pactaba la colaboración de las principales agencias de inteli-

-gencias de estos dos países, pero no solo establecía el intercambio del producto de inteligencia acabado, sino que incluía toda la inteligencia que se recoge, distribuye o produce que tenga que ver con comunicaciones extranjeras, por lo cual se compartía tanto el producto como los métodos utilizados para obtenerlo y conformarlo.

Además, a pesar de que en este momento Canadá, Australia y Nueva Zelanda no estaban incluidas en este acuerdo bilateral, sí que tenían la opción de acceder a dicha información a través de acuerdos bilaterales o con Londres o con Washington. Si Londres quería compartir información con alguna de sus excolonias debía mantener informado a Washington del proceso y de lo que se compartía. Mientras que si era Estados Unidos el que quería compartir información, este intercambio debía ser aprobado previamente por Londres.

Esto cambiaría en la década de 1950, con la realización de ciertas enmiendas al tratado UKUSA. En primer lugar, la inclusión de la NSA en el acuerdo por parte de Washington, siendo la agencia que se ocupa de las comunicaciones, sustituyendo a "Armed Forces Security Agency". Por otro lado, la inclusión de Canadá miembro de pleno derecho, con voz propia y con la capacidad de compartir y recibir información de formar indiscriminada en 1952. Finalmente, en 1956 se incluyó a Nueva Zelanda y Australia en dicho acuerdo como miembros de pleno derecho, pero el contenido de dicho acuerdo es aún material clasificado.

El resultado de la creación de los "Five Eyes" fue la creación de una red de vigilancia global conformada por países angloparlantes en cuyo seno sus organizaciones especializadas en SIGINT, la NSA, el GCHQ, el CSEC, el DSD y el GCSB, colaboraban como si formasen parte de un mismo país. No obstante, el área de acción de cada país y las agencias que lo conforman se dividió por territorios teniendo en cuenta sus prioridades en seguridad nacional y cercanía a otros países.

Sin embargo, esta alianza nació con un adversario marcado, la URSS, en medio de un clima internacional de bloques, la Guerra Fría. En esta competición por no verse sorprendidos por innovaciones tecnológicas, desplazamientos de submarinos u operaciones de contra inteligencia podemos dividir las acciones en dos pilares.

La primera, la parte material, referida al establecimiento de puestos de escucha o satélites, siendo estos últimos claves a partir de 1960. El compromiso de los Five Eyes a la hora de la instalación y el mantenimiento de estos puestos de comunicación que proveyeron de una gran cantidad de información de la URSS y China, pero también de otros objetivos durante la Guerra Fría, fue clave en este tiempo.

Una de las estaciones con más actividad era y es Pine Gap en Australia. Por una parte, eran capaces de detectar lanzamientos de misiles nucleares o la explosión de ojivas nucleares en ensayos tanto en territorio chino como soviético lo que daba información de la capacidad nuclear de estos países, así como en el caso de producirse, dar aviso de una alerta temprana de misil. Por otra parte, estas estaciones ayudaron a hacer un seguimiento de las diferentes innovaciones militares de la URSS o si estaban cumpliendo con los tratados internacionales acordados, como los controles de armas.

La segunda parte, es la referida al software, donde podemos destacar el programa ECHELON que desde la década de 1960 ha interceptado comunicaciones de palabras clave seleccionadas por los Five Eyes a través de los satélites de comunicaciones. Mediante programas muy sofisticados llamados diccionarios, estas conversaciones se clasificaban de acuerdo a esas palabras clave y eran mandadas a analistas. Obviamente, este programa era secreto y no fue hasta después del final de la Guerra Fría cuando se reveló su existencia causando ciertas críticas debido a la invasión de privacidad que podía suponer.

No obstante, las relaciones entre los miembros de los Five Eyes no siempre fueron buenas. En la década de 1980, el conflicto diplomático entre Estados Unidos y Nueva Zelanda debido a que este último país no permitiese la entrada de barcos estadounidenses en sus puertos debido a una política contraria a la energía nuclear derivó en la ruptura del tratado ANZUS y la detención del flujo de la inteligencia estadounidense a este país. Sin embargo, pese a este conflicto, los demás miembros de los Five Eyes siguieron compartiendo información con Wellington demostrando la resiliencia de la alianza frente a desacuerdos políticos.

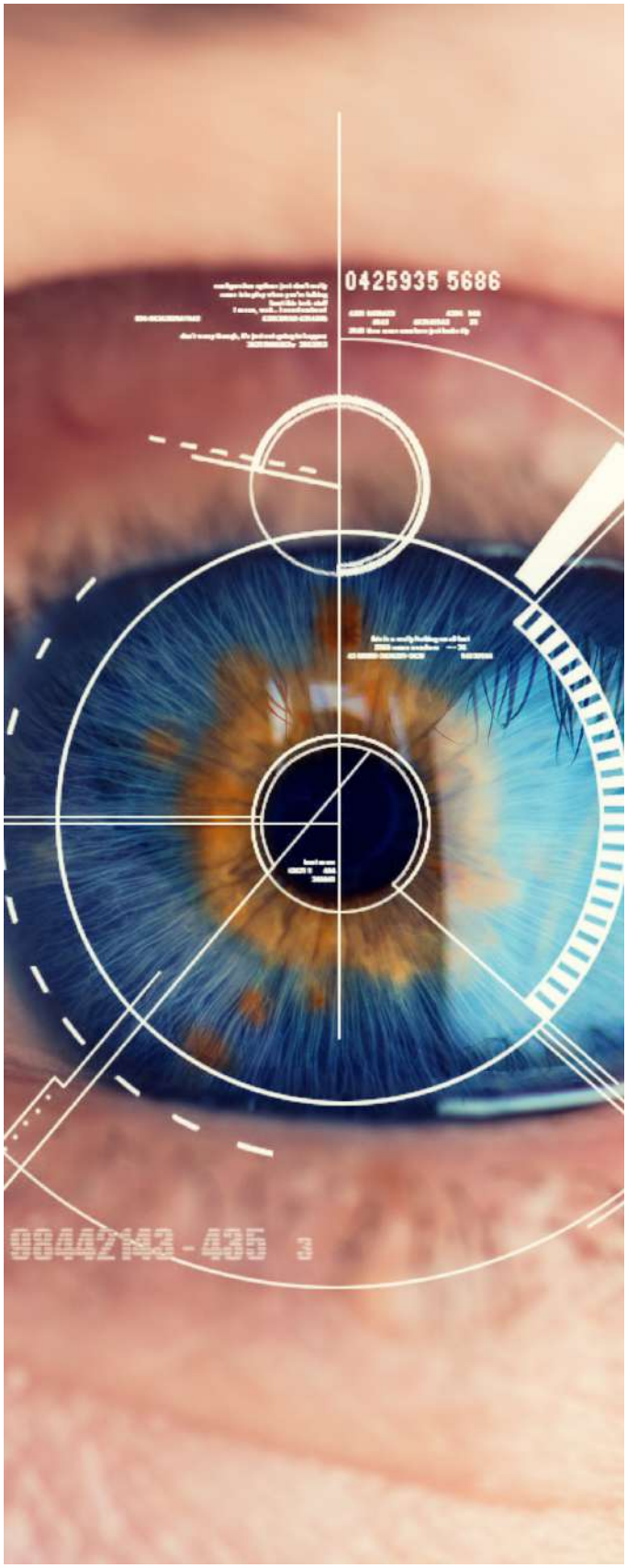
Tras la caída de la URSS hasta la actualidad, los objetivos y roles de los cinco componentes de esta alianza han cambiado radicalmente y a gran velocidad debido al cambio en la naturaleza de los conflictos y amenazas a las que se enfrentaban.

Desde la década de 1990 hasta hoy en día podemos ver cómo han ido apareciendo desafíos que no eran concebibles cuando se creó esta alianza, siendo principalmente tres, el terrorismo, las nuevas tecnologías y la competencia entre países.

Los atentados del 11S y el fracaso en su detención junto con la posterior aparición del ISIS, con sus nuevas formas de captación o el problema de los foreign fighters han supuesto un desafío para la alianza, poniendo en peligro directamente a la ciudadanía de cada país no quedando libre ninguno de los países implicados.

Las nuevas tecnologías como la computación cuántica, los metadata, la IA o el 5 G han provocado una revolución en el mundo de la inteligencia. Antes se necesitaban varias personas y días para analizar la información obtenida y transformarla en inteligencia. Ahora, un ordenador lo hace en segundos dando al analista la posibilidad de analizar grandes cantidades de datos con una gran facilidad

Esto ha supuesto que los Five Eyes se queden anticuados



tecnológicamente y que sea de gran urgencia que inviertan en estas nuevas tecnologías que avanzan a gran velocidad, no solo para poder tener esa superioridad tecnológica que siempre les ha dado la ventaja, sino para poder salvaguardar y encriptar sus propios procesos y comunicaciones. Como expusieron diferentes ponentes en la conferencia Policy Exchange (Policy Exchange UK, 2018), el ciberespacio es el principal reto al que se enfrenta la alianza

Por último, la competencia entre países, principalmente con Rusia y China, pero sin olvidar a los países de Oriente Medio o a Corea del Norte. Esto ha hecho que por una parte la posibilidad de que se produzca un conflicto aumente y por otra parte que los regímenes autocráticos tengan la capacidad de acortar distancias en cuanto a poder con los Five Eyes a la vez que exportan su modelo de gobierno, principalmente en el caso de Pekín como hemos podido ver durante la crisis del COVID-19.

En este contexto, conviene recordar la cooperación que tienen los Five Eyes con países aliados. Dicha cooperación se clasifica en la cantidad de inteligencia compartida y la transparencia respecto a la metodología utilizada o las fuentes. Así, podemos encontrarnos los 8 Eyes o los 14 Eyes donde está incluida España. También debemos destacar la cercana colaboración de esta alianza con Japón e Israel.

No obstante, pese a las diferentes iniciativas políticas que se han dado para incluir a algunos de estos países en la alianza, esto es poco probable debido a las diferencias culturales, a las dinámicas de trabajo establecidas durante más de 70 años y la confianza entre las agencias involucradas que han permitido dejar siempre a un lado las diferencias políticas que hayan podido existir.

Sin embargo, que esta alianza siga siendo puntera en la obtención y elaboración de inteligencia dependerá de una mayor colaboración con países aliados y la inversión en materia de ciberseguridad.

REFERENCIAS

Dittmer, J. (2014). Everyday Diplomacy: UKUSA Intelligence Cooperation and Geopolitical Assemblages. *Annals of the Association of American Geographers,* 604–619.

Miller, P. F. (2015). Rethinking 'Five Eyes' Security Intelligence Collection Policies and Practice Post Snowden. *Intelligence and National Security,* 345-368.

O'Neil, A. (2017). Australia and the 'Five Eyes' intelligence network: the perils of an asymmetric alliance. *Australian Journal of International Affairs*, 529-543.

Patman, A. G. (2021). Small state or minor power? New Zealand's Five Eyes membership, intelligence reforms, and Wellington's response to China's growing Pacific role. *Intelligence and National Security,* 34-50.

Pfluke, C. (2019). A history of the Five Eyes Alliance: Possibility for reform and additions. *Comparative Strategy,* 302-315.

Policy Exchange UK. (27 de Jun de 2018). *The Importance of the Five Eyes in an Era of Global Insecurity.* Obtenido de Youtube: https://www.youtube.com/watch?v=RAjTwZvMhHQ

Walsh, P. F. (2020). Improving 'Five Eyes' Health Security Intelligence capabilities: leadership and governance challenges. *Intelligence and National Security,* 586-602.

Wark, W. (2020). The road to CANUSA: how Canadian signals intelligence won its independence and helped create the Five Eyes. *Intelligence and National Security,* 20-34.

Wells, A. R. (2020). *Between Five Eyes- 50 years of intelligence sharing.* Casemate Publishers.

COMING SOON...

AGENCIA DE INTELIGENCIA ANTITERRORISTA

NERTOM

SEGURIDAD

WWW.ALGHURABA.ORG

EL NEGOCIO DEL RAAS

RANSOMWARE COMO SERVICIO

Marc Rivero López.

Coordinador del máster de CiberSeguridad de La Salle Barcelona, Universidad Ramón Llull.

Si preguntamos al público general por algún tema relacionado con la CiberSeguridad que "le suena de oídas", probablemente la palabra ransomware aparezca en la conversación. Hemos podido observar cómo empresas, usuarios particulares, organizaciones sin ánimo de lucro e incluso gobiernos en todo el mundo, se han visto afectados por este tipo de amenaza. No obstante y por aquello de recoger el contexto histórico de, "De donde puede venir esto" es bueno recordar cuál ha sido la evolución hasta el día de hoy en cuanto a esta amenaza.

El mal llamado Virus de la Policía

Corría el año 2011 cuando empezaron a reportar en distintos medios técnicos y también en los medios de carácter generalista la noticia de un virus que usaba como gancho la imagen de la policía para pedir un rescate económico a cambio de desbloquear el equipo informático. Este malware, una vez ejecutado en la máquina, bloqueaba el acceso a la misma, impidiendo al usuario el poder realizar ninguna acción sin antes pagar un rescate económico que, en las pri-

-meras versiones no solía superar los 150 €, nada que ver, con las cantidades que se están demandando a día de hoy en los ataques realizados con ransomware.

Este "Virus de la Policía", fue bautizado por ese nombre, ya que en sus infecciones, usaba como imagen las distintas policías de cada país. ¿Qué policía mostraba? Pues bien, el malware en cuestión al ejecutarse, conectaba con un servicio de consulta de geolocalización y entonces descargaba el fondo de pantalla con la policía de dicho país para mostrárselo al usuario.

Es curioso, como en algunas regiones donde existía una policía autonómica que tenía competencias sobre otro cuerpo policial dentro del mismo país, este "Virus de la Policía" obviaba tales datos y, iba colocando fondos de policías de ese país de forma aleatoria a la campaña en cuestión para ese momento. Además de usar la imagen de la policía, también usaron en el caso de España, la imagen de la casa real y del Rey emérito para "forzar" al usuario a realizar el pago del rescate que se pedía.

Los modelos de pago aceptados en aquel momento eran Ukash y PaySafe card, ya que otorgaban cierta capa de anonimato para los cibercriminales que recibirían ese dinero. A pesar de que pueda parecer un esquema de fraude complejo, el malware en aquel entonces, año 2011, era bastante inofensivo y fácil de desinfectar con ciertos conocimientos de informática.

Evolución hacia el cifrado de archivos

La evolución natural por parte de los atacantes fue la de, en lugar de bloquear el acceso a la máquina, vamos a cifrar el contenido de los archivos del sistema para que en el caso de que el usuario los quiera recuperar, tenga que pagar un rescate económico por ellos. En las primeras versiones de estos malware's conocidos como ransomware, los cibercriminales buscaban extensiones concretas de archivos en la máquina tales como archivos .doc, .ppt, .xls, .jpeg, .png es decir, documentos ofimáticos e imágenes, que los usuarios pudieran tener guardados en sus ordenadores. El usuario común para aquella época en la que los ransomware empezaron a hacer estragos no realizaba copias de seguridad de sus archivos por lo que cuando se infectaron con este tipo de ransomware, muchos se vieron forzados a pagar.

El esquema de ataque por parte del ransomware no cambió hasta muy recientemente y, este tipo de malware, ha seguido teniendo muchísimo éxito atacando tanto a usuarios particulares, como empresas, como organizaciones sin ánimo de lucro e incluso gobiernos.

Ransomware combinado con malware de tipo gusano

Si nuevamente le preguntamos al público general sobre WannaCry, probablemente el nombre les suene familiar, ya que fue el primer ransomware, que además de cifrar los archivos, tenía la capacidad, de que propagarse de forma automática, por lo que no solamente importaba el "paciente o" de la organización que se infectaba, sino también todas las máquinas de la red local donde esta máquina estuviera ubicada. Os podéis imaginar el drama que supuso en su momento a nivel mundial, las infecciones por el ransomware WannaCry, algunas empresas tuvieron que mandar durante días a sus trabajadores a trabajar a casa.

Intrusiones en las empresas

Los grupos de cibercriminales detrás de estas campañas de infección de ransomware están subcontratando otros equipos de cibercriminales que se encargan de vulnerar tanto empresas, como gobiernos, como distintas organizaciones a las que los desarrolladores de ransomware o sus afiliados, entrarán para cifrar los datos, exfiltrarlos o permanecer allí aprendiendo de como la empresa funciona, para poder extorsionarla.

Del cifrado de archivos al filtrado de información

Una de las últimas tendencias observadas dentro del ecosistema de ransomware ha sido el filtrado de información.

Conforme ha ido pasando el tiempo todas las víctimas de todos los ámbitos han recaído que con una buena política de copias de seguridad pueden evitar pagar cada vez que sus archivos se ven cifrados. Es por eso, que los cibercriminales detrás de estas campañas de ransomware, han decido previo al cifrado de información robar la misma, de manera que si la víctima no paga el rescate de la información, los cibercriminales acabarán publicándola a disposición de todo el mundo de forma gratuita.

Os podéis imaginar qué problema puede suponer para aquellas empresas que tengan cierto "know-how" que se ve publicado y a disposición de sus competidores o bien, aquellos datos de carácter personal como DNI, números de la seguridad social, multas de tráfico, etc, de usuarios ciudadanos particulares. En este nuevo esquema, las víctimas no solo tienen sus datos cifrados, sino que además, se verán publicados en caso de que no paguen el rescate demandado.

Del cifrado y la filtración a la extorsión a terceros

La última tendencia observada por parte de los criminales es la extorsión a terceros que no se vieron afectados por el ransomware sino, que en los datos que le han robado a la víctima han aparecido, correos electrónicos, contratos, en definitiva, datos de otras empresas con las que la víctima ha mantenido contacto y, que por ende, también se podría ver afectada en caso de que este grupo de cibercriminales decidiera publicarlos de manera pública a disposición de todo el mundo.

¿Cómo funciona el servicio RaaS?

Llegados a este punto probablemente el lector se pregunte, que cómo es posible que este negocio sea tan lucrativo y, cómo es posible que se hagan tantas víctimas. El modelo de negocio que se ha construido alrededor de este esquema de ransomware es el de "ransomware como servicio" en el que lo desarrolladores de este tipo de malware, delegan ciertas parte del esquema de ataque a terceros que recibirán un pago u otro dependiendo del número de víctima que consigan realizar. Pongamos un ejemplo práctico, dentro del ecosistema underground, tenemos una serie de cibercriminales especializados en realizar campañas de SPAM que son capaces de saltar cualquier sistema de filtrado instalado en cualquier empresa del mundo. A este tipo de cibercriminales, se les encarga por parte de los desarrolladores de ransomware, la tarea de incluir su pieza de ransomware dentro de sus campañas de SPAM y, por cada víctima que consigan se les dará un porcentaje del dinero total que la víctima pague por recuperar los datos.

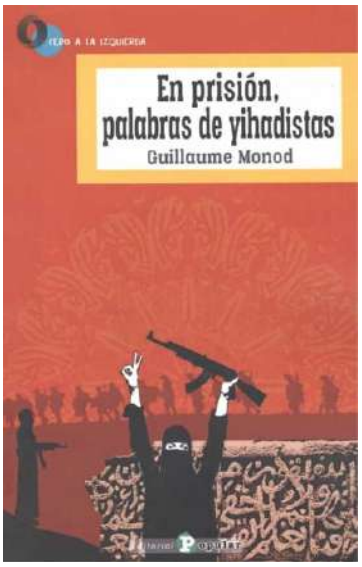
¿Qué parte se llevan del rescate?

La pregunta por parte del desarrollador del ransomware sería: ¿Cuántas víctimas puedes hacer? Para aquellos cibercriminales que puedan hacer un gran número de víctimas se les pagará un porcentaje mayor que suele oscilar entre el 30% y el 65% dependiendo de la familia de ransomware y, de la cantidad de éxito que tenga ese cibercriminal en conseguir víctimas.

Conclusiones

El negocio de los RaaS, "Ransomware como Servicio" radica en la efectividad de propagación del ransomware y en los ataques realizados donde la seguridad perimetral de las empresas se ve vulnerada por los cibercriminales. El dinero que mueve esta industria ha ido creciendo de forma exponencial desde su nacimiento y cada vez existen más familias de ransomware que operan en este sentido. Desde las empresas de seguridad, los centros de respuesta ante incidentes de cada región y, organismos oficiales como Europol, existen iniciativas para luchar contra este tipo de amenaza dentro de la ciberseguridad. Algunas de las recomendaciones a seguir por parte de todas las posibles víctimas es mantener al día los parches de seguridad del software que se ejecuta en la organización, aplicar distintas capas de protección, enfrentar tus defensas a estándares como el MITRE ATTACK y, en definitiva las guías de buenas prácticas desarrolladas por organismos oficiales, en el caso del ámbito nacional, el Centro Criptológico Nacional.

TINTA IMPRESCINDIBLE



Título: En prisión, palabras de yihadistas

Autor: Guillaume Monod

Editorial: Popular

Tras los ataques de París de 2015, apareció una nueva categoría de detenidos en grandes cantidades en las cárceles francesas: el yihadista, un soldado de Daesh. A diferencia de las investigaciones policiales y judiciales, que buscan reunir hechos y establecer pruebas, este libro examina los ideales y fantasías con las que estos luchadores justifican su compromiso en un viaje donde se mezclan el idealismo utópico y la peor violencia. Para escuchar las palabras de este tipo especial de detenidos, es necesario desvincularse temporalmente de cualquier juicio moral. A lo largo de sus entrevistas, Guillaume Monod, psiquiatra infantil, señaló que la relación de los yihadistas con la religión no es tanto teológica o política como mitológica, porque el Estado Islámico encarna un mito que tiene sus raíces más en la geopolítica contemporánea que en la milenaria historia del Islam. Una pregunta recorre este libro: ¿Qué impulsa a estos jóvenes franceses a marcharse, a riesgo de su vida, a un país del que no saben nada, ni incluso el idioma?

CONTRA-NARRATIVA

WWW.ALGHURABA.ORG

ASPECTOS PSICOSOCIALES

SUBYACENTES A LA RADICALIZACIÓN YIHADISTA EXTREMA

Andrés López Franco

Doble Grado en Ciencias de la Educación; Director e Instructor de Seguridad Privada Acreditado. Sargento (R.H.) del E.T.

Radiojai

Las narrativas para la radicalización, ya sean yihadista o de cualquier naturaleza, buscan llenar el vacío de ilusión, justicia, verdad y esperanza que la pobreza y la violencia en sus múltiples estados le han arrebatado al ser humano, en un primer momento se busca alguna verdad en estos discursos que reconforte sentimientos y desesperación, luego buscará en la arenga de sus líderes alcanzar su parte de venganza; pasando de ser seres humanos a transformarse en seres completamente deshumanizados en casos de extrema radicalización.

Tras esta reflexión introductoria, siempre discutible, pero con un fuerte respaldo bibliográfico y documental de expertos en esta materia, pretendo mostrar algunas premisas psicosociales yihadistas impregnan las narrativas yihadistas y que conducen a la radicalización extrema de sus "simpatizantes", un punto de "no retorno" que es interesante contemplar en cualquier análisis que hagamos sobre el fenómeno de la radicalización yihadista y sus contingencias.

Tendríamos que aproximarnos en primer lugar al caldo de cultivo que subyace tras el pensamiento colectivo de la Yihad Global, investigar exhaustivamente en qué entornos se generan esos pensamientos, y por qué; abordar tantos contextos como están actualmente identificados por las múltiples entidades de inteligencia centradas en este proble-

-ma extendido ya de forma alarmante. Partir de axiomas como que el éxito de la radicalización más extrema está en identificar entre los simpatizantes a la causa, a los individuos más permeables a esta lluvia ácida de conceptos que, suministrados en su medida, transformarán a un ser humano en un asesino sin consciencia, facilitará poder aportar soluciones concretas y enfocadas.

Una entre muchas premisas psicosociales importantes desde las que ubicar los contenidos de este artículo (haciendo una adaptación de lo que Arnold Mindell, en 1995 recogía en su obra: Sitting in the fire), es que: Si no hay salidas legítimas al odio, a la opresión y a las hostilidades, al hambre, a la miseria, a la explotación en todas sus execrables formas... estas tomarán rutas ilegítimas, y en el peor de los casos el camino elegido costará vidas.

Pero, ¿podríamos discernir en qué medida los terroristas radicalizaron sus comportamientos consecuencia de la interiorización de un discurso violento?, o ¿cómo se combinaron, cuándo, y de qué modo intervienen el resto de mecanismos psicosociales existentes para la radicalización y transformación de un/a simpatizante, en un/a terrorista?. (Adaptación hecha al contenido de Leuprecht et al, 2010).

Cuando pretendemos establecer una correlación entre los aspectos psicosociales y la influencia de contranarrativas como herramientas atenuantes de procesos: psicológicos, políticos, sociológicos, religiosos, de parentesco y pertenencia, de arraigo, etc., que giran en torno al fenómeno de la radicalización, caemos en la cuenta de la gran variable humana que gira en torno a la activación y desactivación de los procesos psicosociales que acompañan a toda radicalización. (Con este artículo no se pretende detallar lo que requeriría un manual de análisis y estudios de caso que justifiquen la conexión entre ambos factores, sino abrir una puerta al campo de la investigación con fines estratégicos y defensivos, donde se añada el campo de los factores psicosociales como activadores o desactivadores de conflictos).

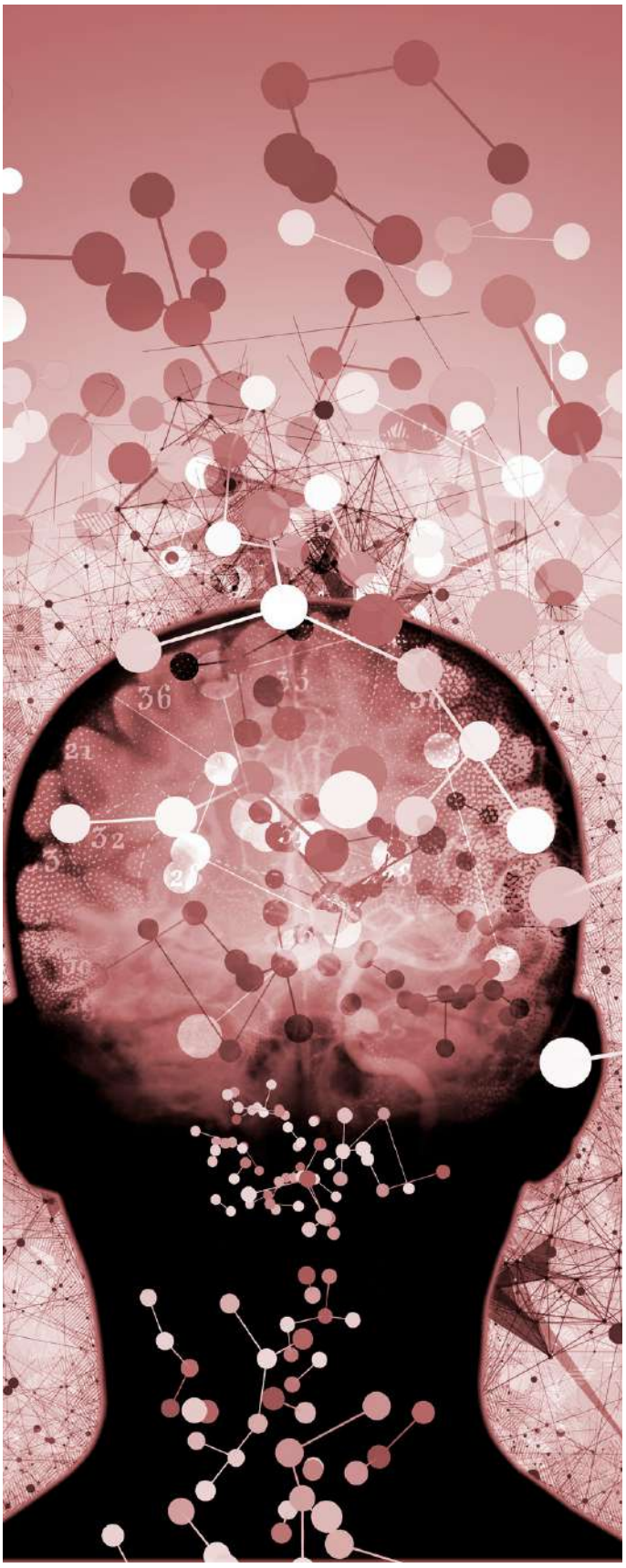
Profundizando un poco más en los aspectos psicosociales que estamos abordando, es importante observar la variable religiosa, siendo necesario detenerse en el sentimiento de venganza, o "revancha", para seguir preguntándonos: ¿qué subyace en la mente de estos terroristas que justifican la muerte de inocentes, e incluso la suya propia, basándonos en un texto sagrado?.

Son conocidas muchas citas religiosas en textos de culto y oración que han influido en cierto modo en la cultura popular, llevando un mensaje de revancha manifiesto: *"¡Qué no crean los infieles que van a escapar! ¡No podrán! ¡Preparad contra ellos toda la fuerza, toda la caballería que podáis para amedrentar al enemigo de Dios... Si, al contrario, se inclinan hacia la paz [si aceptan el Islam], inclínate tú también hacia ella..."* (Sura 8:59-61). *"...Y, si se apartan, sabe que Dios desea afligirlos por algunos de sus pecados"* (Sura 5:49). *"...¡Creyentes! [musulmanes] ¡No toméis como amigos a los judíos y a los cristianos!. Son amigos unos de otros. Quien de vosotros trabe amistad con ellos, se hace uno de ellos. Dios no guía al pueblo impío"* (Suras 5:51). Son solo algunos ejemplos que también encontramos en la religión cristiana, véase en Levítico 24:20 donde se recoge el conocido *"....ojo por ojo y diente por diente".*

Según trabajos publicados de psiquiatras, psicólogos y facilitadores de procesos conflictivos, consultados para desarrollar estos contenidos: *Cuando buscamos la revancha, estamos convencidos de que tenemos algún tipo de justificación divina para nuestros actos. Este sentimiento de "justicia" transforma la violencia crónica en una especie de "lucha religiosa contra los que hacen el mal"*, (en Mindell, A.1995). En alemán, "revancha" se dice "Rachsucht", que traducido literalmente significa: "adicción a la furia" . En ocasiones el "adicto a la furia" necesitas más, y las consecuencias suman muchos días de terror para el recuerdo: 11-S, 11-M, 7-J...

Para concluir, destacaría la necesidad de reforzar la presencia de perfiles especializados en analizar los enfoques psicosociales de forma transversal al trabajo de analistas de inteligencia y especialistas en defensa y seguridad en los equi-

-pos que trabajan con contranarrativas gubernamentales, de choque, o alternativas, pues este enfoque posibilitaría tratar el conflicto desde su propia naturaleza humana, sin perder de vista las múltiples causas psicosociales que subyacen tras el deseo de venganza.



REFERENCIAS

Leuprecht, C., Hataley, T., Moskalenko, S. Y Mccauley, C. (2010). Narrativas y contranarrativas para la Yihad Global: Opinión y Acción. En Akerboom, E. (Coord.), *Contrarrestar lasNarrativas Extremistas Violentas, Coordinador Nacional de Contraterrorismo* (Nctb), Universidad de Leiden (La Haya) 58-71.

Kohut, H. (1985). *Auto-psicología y humanismo: reflexiones sobre un enfoque psicoanalítico*. W.W. Norton.

Lewin, K. (1972). *Necesidad, fuerza y validez en campos psicológicos.* En .P. Hollander and R.G. Hunt (Eds.), *Contribuciones clásicas a la psicología social.* Oxford University Press.

Mindell, A. (1995). *Sentados al Fuego.* Lao Tse Press, Portland, Oregon, EUA.

Miravitllas, P. E. (2015). *Hacia una tipología de Contranarrativas frente al Extremismo Violento*. Universidad de Barcelona.

-Nora F. y Nilda S. (2008). *"Dinámica de la humillación en la violencia".* Jornadas desarrolladas por el Instituto Internacional de Sociología Jurídica de Oñate, España. 10 y 11 Abril, 2008.

Máster en Comportamiento no Verbal y Detección de la Mentira

Descubre el Meta-Procotolo SAVE de Análisis de Conducta.

Especialízate en el Nonverbal Behavior Analysis Matrix, método de análisis de comportamiento no verbal utilizado por la Policía Nacional Española.

Únete a nuestra 16ª promoción y a los cientos de profesionales que han mejorado su carrera con este máster.

Consigue tu título de master de la **Universidad a Distancia de Madrid.**

www.comportamientonoverbal.com

Behavior & Law

Behaviora & Law Corp. 600 Cleveland St. Clearwater. Florida. USA

Fundación Universitaria Behavior & Law. Simon Hernandez, 65 Móstoles. ESPAÑA

TERRORISMO

WWW.ALGHURABA.ORG

PALABRAS SECUESTRADAS

YIHAD

David Garriga y Ariadna Trespaderne.
Criminólogos.
Presidente y Secretaria General de la Comunidad de Inteligencia y Seguridad Global.

Como consecuencia del surgimiento de determinadas organizaciones terroristas, occidente posee un preocupante sesgo interpretativo sobre el concepto “yihad”. Esta palabra sufre de una imagen descontextualizada y malbaratada fruto de los grupos extremistas que han hecho del término su razón de ser, por y para morir. Dicha descontextualización ha sufrido una cierta vulgarización del término, acompañado, en algunos casos, de fuertes distorsiones (García, 2009). Ciertamente la ciudadanía y algunos teóricos clásicos lo asocian con la guerra santa (Cook, 2015), pero en realidad, la semántica indica que no existe un sustrato con la guerra santa como tal. Sus principales interpretaciones se dirigen a "esfuerzo" y "guerra defensiva", y no toda guerra defensiva cumple las condiciones para etiquetarse como "yihad".

Quiénes suscriben, lejos de ser teólogos o exponentes del pensamiento islámico, quieren insistir en la importancia del uso de la palabra, pues, en procesos de radicalización violenta, donde el fanatismo es el constructo cognitivo básico para segmentar a las personas entre dos mundos, nada es al azar. Pues como sabemos, las palabras son armas de destrucción masiva y esta, entre otras, se ha ido diluyendo entre la narrativa terrorista hasta impregnarse en nuestro imaginario colectivo. Este hecho, exige revivir su significado original y contrarrestar a su vez los discursos radicales. Tal y como Bockstette (2010) indica el terrorismo de etiología yihadista emplea en muchas ocasiones el término jihad terrorism porque está "aparentemente motivado por una interpretación extrema del islam y sus practicantes consideran el uso de la

violencia como un deber divino o un acto sacramental" (p.10) en confrontación al orden occidental, entre otros.

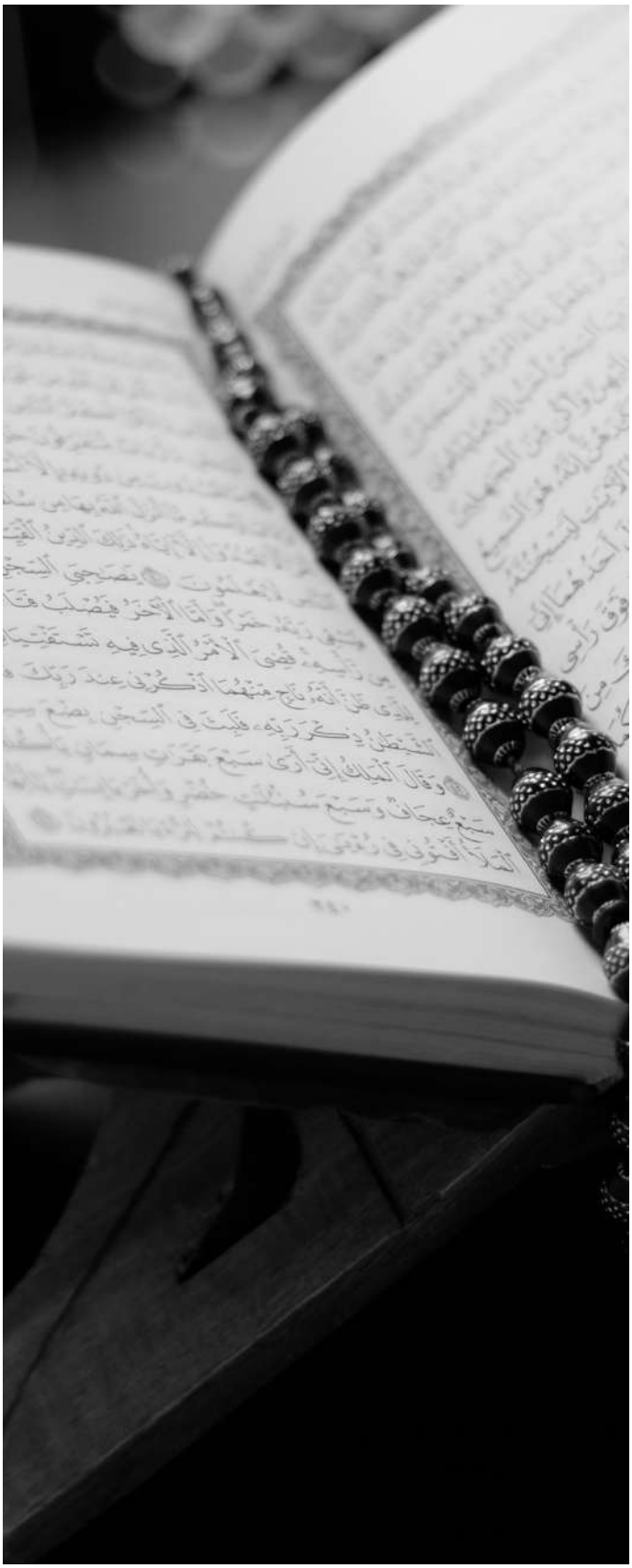
Por eso, la narrativa es tan importante, porque es una secuencia de hechos y términos vinculados entre sí en una línea argumental (Lawler, 2002) y el uso de la palabra ligada a la realidad es deliberadamente simplificada en casos como este. De hecho, en el terrorismo de la etiología yihadista existe una interpretación radical y manipulada de las leyes islámicas y todos los términos que las rodean (Jan, 2009). En consecuencia, es una crónica interpretativa ideal que permite convencer a perfiles potenciales radicalizados, enaltecer la ideología extremista y solidificar sus fieles, alterar la visión del exogrupo y, sin duda, justificar acciones violentas (Archetti, 2013).

La palabra yihad apareció en occidente no hace mucho tiempo relacionada con este fenómeno. Como advertimos, entre sus definiciones quizás dos han sido las más extendidas entre occidente. Por un lado, aquella que relaciona el concepto yihad con una "guerra santa" de los que abrazan el islam contra los infieles considerándola como el sexto pilar del islam. Y, por otro lado, como sinónimo de "esfuerzo" para la superación de las dificultades y tentaciones en el día a día de todo musulmán. De hecho, el término yihad se refiere a la obligación que tiene el musulmán de esforzarse para instaurar en la tierra la palabra de Dios, el islam, combatiendo si es preciso. Este tipo de obligación ha sido controvertida desde los primeros días de la expansión del islam, pudiendo abarcar desde la persuasión oral y ejemplarizante del Profeta en la ciudad de la Meca hasta la guerra al final de su vida en la ciudad de Medina (Gómez, 2019).

Aunque el significado más común de yihad es entendido como un esfuerzo en el camino hacia Dios, un esfuerzo espiritual hacia la propia perfección y la lucha contra el egoísmo. (Tamayo 2009) muchas veces, desde sectores radicales y posturas integristas se ha presentado este concepto unido a la "guerra santa". Pero insistimos que tal lucha en ningún caso es violenta y, en todo caso, en legítima defensa hacia las agresiones exteriores.

Así, aparecen dos tipos de yihad, por un lado, "Yihad Mayor" (Yihad al Kabar), referida al esfuerzo personal del individuo contra sus propias pasiones, ese sacrificio por lograr una vida espiritual perfecta y armónica en la lucha contra las fuerzas del mal que anidan en cada persona y contra las injusticias que se producen en cada sociedad. Y, por otro lado, "Yihad Menor" (Yihad al Askar) referente a la acción de todo musulmán con el objetivo de expandir el islam por el mundo (Garriga, 2015).

En cuanto a los diferentes ideólogos que han tratado este concepto encontramos los que se posicionan en defender yihad como "guerra santa" y los que la definen como "esfuerzo" o "guerra defensiva". Entre los primeros hallamos a **Ibn Taymiyya,** el cual dictó una fatwa en donde exponía como un deber religioso el combatir contra las sectas islamistas que incumplieran alguno de los pilares del islam. Según este teólogo, los musulmanes, tras escuchar la palabra del Profeta Muhammad para seguir el islam, debían combatir contra los infieles y a cambio recibirían el mejor de las recompensas, el paraíso. Otro de estos ideólogos está **Mawlana Sayyid Abu al-Mawdudi** (1903-1979), que bajo la creencia de que Dios es el legislador supremo y solo depende de él regir los asuntos de los humanos. Sostiene que la yihad bélica es justificable en cuanto el islam, como sistema integral, tiene el objetivo de eliminar los demás sistemas del mundo. Se opone a la diferencia entre yihad ofensivo y defensivo y cree que toda persona que no responde al yihad es considerado no-creyente. **Hassan al-Banna** (1906-1949), fundador de los Hermanos Musulmanes, es una sociedad muy conservadora dedicada a resucitar el califato islámico sobre todas las naciones y extender su poder al planeta entero. Basa sus creencias en el deseo de regresar a los preceptos del Corán y rechazar las influencias que puedan venir de occidente. Al-Banna utilizaba el siguiente lema para defender las ideas de los Hermanos Musulmanes: "Alá es nuestro objetivo, el Profeta nuestro líder, el Corán nuestra constitución, la yihad nuestro camino y la muerte por Dios nuestro objetivo supremo". Otro ideólogo que defendió el concepto bélico de la palabra yihad fue el egipcio Sayyid al-Qutb (1906-1966).



Seguidor acérrimo de los Hermanos Musulmanes, el cual pasó los últimos años de su vida en la cárcel, donde fue ejecutado. Su principal idea es que como los gobiernos occidentales están usurpando la autoridad de Dios, a través de la yihad se debe luchar contra estos gobiernos déspotas (Garriga, 2015).

Entre los segundos, o los ideólogos que defienden el concepto yihad como esfuerzo o guerra defensiva encontramos a **Muhammad Abduh** (1849-1905). Siempre abierto al diálogo entre las tres religiones monoteístas. Definió el yihad no como una guerra sino como un esfuerzo por vencer las dificultades de todos los musulmanes y con el fin de defender la verdad y la difusión del islam con el alma y los bienes, nunca con las armas. Creía que el islam estaba sufriendo una decadencia interna y necesitaba una reforma, para esta renovación ayudaría mucho la influencia de occidente y separar la política de la religión. Definía el islam como una religión de paz y de perdón, la guerra no es para convertir a alguien al islam ni para vengarse, sino que solo ha de usarse como legítima defensa de las agresiones. Otro defensor de esta definición fue **Mawlana Sayyid Abul al-Mawdudi** (1903-1979), pues mantenía una tendencia radical a favor de la guerra, concibió el yihad como una lucha dentro de la comunidad musulmana encaminada a su reforma. Esta transformación había de darse siempre de una manera gradual y conjuntamente con la educación, nunca de manera brusca y por la fuerza. También **Abdelazziz al-Tha'alibi** (1874-1944), quién basaba su creencia en defender que una de las principales virtudes de los musulmanes es la tolerancia, sobradamente demostrada en varias suras del Corán, suras que el fanatismo ha llevado a interpretaciones alteradas e interesadas de los textos para poder justificar la llamada de los musulmanes a luchar (Tamayo, 2009).

Cierto es de la existencia en el Corán de la palabra yihad referida como guerra. Pero no toda guerra se ajusta al concepto de yihad, no todo vale. Las condiciones que debe respetar toda acción bélica para considerarse yihad y que constan en el Corán, en la sunna del Profeta y en las costumb-

-ostumbres de los compañeros del profeta y que muy bien detalló Averroes en el siglo XII en su obra jurídica Bidāya (1168) son, entre otras (Haya, 2003): Está prohibido matar a no combatientes. Queda prohibido asesinar a niños y mujeres (con una excepción y es cuando la mujer o el niño participan de manera activa en la lucha, pues en ese caso son considerados soldados). Tampoco se permite matar a personas vulnerables o con características especiales de cualquier tipo que les impida participar en la lucha, es decir, personas mayores, con diversidad funcional, trastornos mentales, ermitaños, representantes religiosos como los monjes, ni personas de otra religión. Se prohíbe matar a comerciantes, mercaderes, contratistas y similares que no tomen parte en la lucha. Está prohibido torturar a los enemigos y mutilar sus cuerpos. Incluso se prohíben acciones como talares árboles frutales, sacrificar ovejas o ganado si no es para alimentarse ese mismo día o destruir edificios, aunque estén deshabitados.

Si comparamos estas normas para realizar la yihad bélica con la mayoría de grupos terroristas de etiología yihadista de los últimos tiempos, vemos que no cumplen apenas ninguna de las premisas, por lo que ni siquiera se les tendría que llamar yihadistas (los que hacen la yihad) ni a su guerra, yihad. Es muy importante tener en cuenta la realidad histórica, ya que la elaboración de la idea de yihad como 'guerra' en relación con el infiel se fundamenta en las primeras etapas coránicas y primeras conquistas islámicas, no en la actualidad y sobre todo debe desmitificarse el concepto de «guerra santa». Este tiene su origen en los cristianos, quiénes lo elaboraron cuando se sentían amenazados por los musulmanes.

Queda claro que el concepto yihad ha sido empleado por parte de las organizaciones terroristas para conseguir una supuesta transformación revolucionaria y belicosa. Esta palabra sigue siendo utilizada para legitimar el uso de la violencia y crear un orden ancestral muy alejado de lo que el yihad es para la *umma.* Esta palabra, tan instrumentalizada para legitimar la violencia, no puede ser entendida de ningún "modo como ellos lo plantean. La contranarrativa es nuestra mejor aliada para deconstruir estos conceptos y con estas líneas deseamos que quede patente que esa yihad secuestrada a la que se refieren estos grupos no promueve, en realidad, una causa justa, tal y como hemos podido analizar en los párrafos anteriores pues no respeta los códigos originales de la tradición. Ninguna masacre perpetrada por ellos se ajusta al llamamiento del yihad.

REFERENCIAS

Archetti, C. (2013). Narrative wars: Understanding terrorism in the era of global interconnectedness. En A. Miskimmon, B. O'Loughlin y L. Roselle (Eds.), *Forging the world: Strategic narratives and international relations* (pp. 218-245). University of Michigan Press.

Bockstette, C. (2010). *Jihadist terrorist use of strategic communication management techniques.* DIANE Publishing.

Cook, D. (2015). *Understanding jihad.* University of California Press.

García Sanjuán, A. (2009). Bases doctrinales y jurídicas del yihad en el derecho islámico clásico (siglos VIII-XIII).

Garriga, D. (2015). *Yihad.* Comanegra

Gómez, L. (2019). *Diccionario de islam e islamismo.* Trotta.

Haya, V. (2003). Siete aspectos de la violencia en las fuentes islámicas. Justificaciones apócrifas y auténticas. Castellón, ESP.

Jan, M. (2009). Political terrorism under the flag of media. *A research Journal of South Asian Studies, 24*(1), 38-51.

Lawler, M. (2002). *Narrative in social research.* En T. May (Ed.), Qualitative research in action (pp. 242-259). Sage.

Tamayo, J. J. (2009). *Islam, cultura, religión y política.* Trotta.

ENTREVISTA

WWW.ALGHURABA.ORG

SELVA OREJÓN

CONSULTORA EXPERTA EN CIBERSEGURIDAD. PERITO JUDICIAL ESPECIALIZADA EN IDENTIDAD DIGITAL Y REPUTACIÓN. FUNDADORA DE ONBRANDING.

Entrevista de Antonio Martín López

Selva Orejón, en twitter @selvaorejon, es perito judicial especializada en Identidad digital y reputación. Licenciada en Ciencias de la Comunicación por la Universitat Ramon Llull y Diplomada en Business Organization and Environment, University of Cambridge, e Inteligencia al Servicio del Estado y la Empresa, ejerce como profesora en la Universidad de Barcelona UB en el Máster de Ciberseguridad, impartiendo Ciberinteligencia – OSINT, y en la Escuela de Policía de Catalunya, (Ciberinvestigación y Protección de la identidad digital). Su empresa, onBRANDING cumple 14 años especializada en gestión de crisis de reputación online para celebridades como clubes de 1a división de fútbol, agentes de futbolistas y jugadores; empresas y ciudadanos anónimos. Tiene el privilegio de dar clase de las mismas especialidades a la Policía de Israel, y en el Consejo General del Poder Judicial.

1. ¿Qué te llevó a crear onBRANDING? ¿Y a qué os dedicáis?

Estudié ciencias de la comunicación, pero la especialidad de publicidad y relaciones públicas, y mi tutora es quizás la mejor analista de inteligencia empresarial que conoceré en mi vida. Mis seminarios fueron de gestión de crisis corporativas y marca

personal, y ahí empieza la conexión. Cuando me fui a vivir a Berlín, en el año 2006, Alemania acogía la mayor red social de Europa, StudiVZ.net, y en 2007 vivimos la mayor crisis de reputación que una empresa puede tener, y más allí. La prensa nos asociaba con el régimen neonazi, por parte de los fundadores, esto fue una estocada bestial, y más con mis orígenes de ambos apellidos judíos, imagínate qué duro fue para mí ser la Country Head de España y LATAM, con un rumor así sobre los fundadores. Un desastre.

Luego eso pasó a un segundo término porque nos compró el grupo Holtzbrinck y ahí cambió todo. Cambios brutales internos, una rueda de prensa de presentación, y fue ahí cuando la ciberseguridad impactó en mi vida de cara. Atacaron nuestra base de datos y quien lo hizo pidió un rescate, se le pilló e ingresó en prisión, en una semana se había suicidado. Y... ¡booom! Otro escándalo sobre nosotros. Esto me hizo pensar que si estaba pasando en Alemania, también iba a pasar en España y en todo el Mundo, así que fue mi primera incursión de lleno.

Sobre onBRANDING, el nombre lo propuso una persona muy especial para mi, y significaba dar el paso a poner en práctica de forma profesional todo lo que mis amigos, familiares, conocidos y ya personas de internet me pedían. Ayúdame con mis redes sociales, qué es esto de internet para darse a conocer, cómo protejo mis cuentas, qué debo hacer para ser más visible en ... sitios... En el fondo fue traer mucho conocimiento de Alemania, de trabajar en una start up, y las cosas como son, mis viajes a Estados Unidos e Israel siempre han sido de lo más provechosos. De hecho, onBRANDING ha ido virando, de la parte más de gestión de crisis pura y dura a tener que aplicar cada vez más técnicas de ciberinvestigacion e inteligencia, primero de mercado y ahora de todo tipo. Pienso que en nuestra vida digital somos muy confiados. *¿Es ignorancia? ¿Pensar «a mí no me va a pasar»? ¿Qué opinas?* Es naïf al 100%, pero es humano y entendible. No podemos conceptualizar algo que no podemos imaginar, y si no vemos un ejemplo, no pensamos ni que exista ese mal. Y eso es bueno en el fondo, no hay que culpar a quien piensa que los demás son como él. Aquí es un «se cree la oveja que todas son ovejas, y no ve lobos entre ellas», eso quiere decir que hay más buenos que malos, por eso sigue siendo rentable delinquir.

2. ¿Qué es la Reputación Digital?

La Reputación Digital es tu credibilidad o la de tu empresa en Internet, pero lo podríamos definir como la suma de las percepciones que generamos en una persona, un grupo de personas, o en la opinión pública. Y por supuesto no se puede gestionar, nos funciona como en minority report, pero sí podemos gestionar nuestra comunicación y nuestras acciones, y con suerte, la percepción se modificará. Nosotros la protegemos a través de la vigilancia de la reputación online, la monitorización activa así como a través de la gestión de las crisis reputacionales que se produzcan.

Empecé hace años a realizar también peritajes para la cuantificación de la pérdida reputacional de una marca personal o empresa. Porque detrás de una pérdida reputacional siempre hay una pérdida económica.

Para tomar las riendas de una crisis reputacional, una de los principales herramientas con la que debes contar es con el informe pericial por pérdida reputacional. Nuestro trabajo es ser la fuerza de apoyo que calcule y defienda a tu empresa o a tu marca personal del ataque de desprestigio que estés sufriendo. La defensa de la reputación corporativa y delitos contra la intimidad requiere de profesionales especializados en el área. Diferenciar conflictos entre la libertad de expresión e información y la protección del derecho al honor, a la intimidad y a la propia imagen es nuestra especialidad.

3. En noviembre se cumplirán dos años de la publicación de tu libro "IDENTIDAD DIGITAL", ¿qué podemos encontrar en él?

Para mí es una guía necesaria para cualquier profesional entre cuyas tareas figure la elaboración de inteligencia así como la realización de peritajes de identidad digital. Sirve para aprender a proteger la reputación digital y descubrir las herramientas para defender a una empresa o persona de los posibles ataques que pueda recibir su imagen en la Red. En él hay muchas herramientas, estrategias y documentación para analizar y protegerse de la pérdida de identidad digital y sus ataques en la Red.

4. Siendo la ciberinvestigación otra de tus especialidades, ¿qué opinas de la gestión de las RRSS en la actualidad, desde un enfoque de falta de privacidad real de cara a los usuarios?

La ciberseguridad también tiene unas consecuencias emocionales que pasan desapercibidas. Existen ataques en los que sobre todo el objetivo no es una empresa sino una persona y ahí la privacidad es clave. En la ciberseguridad hay mucho más en juego. En mi despacho trabajo con 19 psicólogos que ven cada día de su vida cómo es el tener una situación de estas características. Hay casos extremos de stalking: de acoso constante y continuado en redes sociales contra una sola persona. Uno de los clientes lo sufre desde hace cinco años y medio. Recibe desde diferentes cuentas en redes sociales acoso, e incluso fotos del interior de su domicilio (...). El único objetivo es desestabilizar emocionalmente. Empezamos a sospechar que detrás hay una empresa contratada para ello. Digamos que el motivo principal [de muchos ciberataques] es el económico, pero el criminal como tal se está empezando a colar en la sociedad de una manera muy inconsciente. No solo somos muy inconscientes a la hora de protegernos. También a la hora de atacar. Y es porque todavía no ha llegado el mensaje desde un punto de vista emocional. O te ha pasado algo muy gordo a ti o a alguien cercano a ti, o este mensaje no llega.

Pero la identidad, también la de los individuos, es más relevante que nunca en el mundo digital. La identidad trasciende el concepto de seguridad. Una identidad ya es un activo de una compañía, no es un sistema de seguridad que tengas que controlar con una lista de permisos. Es un activo a tener en consideración para prácticamente todo.

5. ¿Qué debemos hacer para estar seguros en un mundo digital?

Formación, formación, aceptación, formación y más recursos. Todavía hace falta "más formación emocional" para conseguir un internet seguro para todo el mundo. Hay necesidad de más formación, pero no solo formación tecnológica: también en materia de privacidad y de formación emocional. Cuando hacemos formaciones con los psicólogos con los que trabajamos, una de las cosas a las que le damos muchísima importancia es estimular la empatía. Todos somos seres relacionales y queremos relacionarnos, pero estas relaciones tienen que ser en condiciones de seguridad, respeto y en compromiso con la privacidad del otro.

Algunas de las actividades que podríamos hacer, intentar monitorizar todo el contenido relacionado con la empresa para evitar así sorpresas desagradables. Cabe recordar que lo más preciado para los ciberdelincuentes es la información personal, incluyendo datos bancarios, de tarjetas, etc, y que la forma de ganar dinero con ello es la venta en la deep y dark web. Muchas de esas empresas no saben todo lo necesario sobre ciberseguridad. Por ello, nos da las claves primerizas para empezar a tener un negocio seguro de ciberataques o de hackeos.

- SEGURIDAD DEL PROPIO DISPOSITIVO: antes de nada es imprescindible tener seguro el aparato desde el cual se va a trabajar. Desde el cual la empresa ofrece su servicio.

- SEGURIDAD DE LAS COMUNICACIONES: aunque parezca que no es importante, es de vital importante tener cierta seguridad en aspectos como dónde está conectado tu WiFi, pues eso da información valiosa.

- COMPORTAMIENTO DEL USUARIO: la más importante. Es necesaria la formación de las personas para ser capaces de detectar una mentira. Aunque pensemos que tenemos la mejor seguridad del mundo, nos pueden colar un engaño en cualquier momento, haciéndose pasar por una entidad bancaria por ejemplo.

6. ¿Tiene algún símil un ataque a la Reputación Digital con un bombardeo de narrativas de etiología yihadista?

Completamente, se utilizan algunas de las técnicas SEO de posicionamiento de contenido para imponer el relato, igual que en cualquier narrativa, necesitaremos contra narrativa, técnicas de posicionar imágenes, videos, texto... por encima de los resultados de los "competidores" por la atención de la audiencia. De hecho, en toda campaña de comunicación, el objetivo siempre puede ser positivo o negativo, igual que en una campaña de desprestigio. Es sabido que existen agencias propias de comunicación de grupos terroristas que son las encargadas de hacer llegar el mensaje de la forma más eficiente, al servicio de los intereses de los líderes y del objetivo de la organización. Una muy buena ejemplificación se ve en el reportaje Terror Studios de 2016, emitido por Movistar TV.

7. ¿Cómo podemos prevenir digitalmente hablando la difusión de narrativas extremistas en las RRSS?

Es imparable, pero las plataformas sociales pueden hacer mucho. Filtrar por palabras clave, por IP, por zona geográfica, mediante fingerprinting... y por supuesto colaborando con las agencias de inteligencia de cada país. Es vital la colaboración público privada, y por supuesto y especialmente la colaboración de ciudadanos convencidos de mantener el orden público, estos mismos pueden avisar a las plataformas mediante denuncias de perfiles, y sus contenidos. Hay una tendencia a creer que este trabajo de detección es más tecnológico, pero la realidad es que debe ser mixto, humano y tecnológico, y de aquí que la clave en las próximas actuaciones es poner el foco en el cyber humint.

8. ¿Qué opinas sobre analistas en el campo de la ciberinteligencia que tienen acceso a contenidos críticos y los difunden creando una alarma social?

Flaco favor hacen, no puedes anteponer el ego, o la necesidad de difusión de tu marca personal a los intereses comunes. Se han dado ocasiones en las que ha sido importante llamar la atención a los propietarios de esos perfiles incluso con correctivos internos en caso de ser funcionarios públicos o colaboradores cercanos a agencias de inteligencia.

9. ¿Qué consecuencias puede tener para la sociedad la desinformación que tanto se difunde mediante RRSS y plataformas como Whatsapp, Telegram y otras sin contrastar?

Hay consecuencias sociales, tanto para empresas como para ciudadanos y también para personajes públicos como políticos,

y las campañas de desinformación pueden acabar afectando a la opinión pública, de forma económica y por supuesto psicológicamente, cuando se usa la desinformación contra una persona.

Aunque no hay datos oficiales, la desinformación está en aumento y ya se están consagrando servicios de creación y alimentación de infraestructuras de difusión de contenidos manipulados a merced de un objetivo comunicativo. Hay incluso deep fakes de audio, si se trata de un famoso, la voz puede conseguirla en internet, pero se están dando casos, donde se suplanta la identidad de alguien con cierta credibilidad para dar la máxima veracidad. Le llaman por teléfono con cualquier excusa y cuando ya han conseguido su voz durante unos minutos ya pueden elaborar el plan para engañar a alguien. Saben que con la voz ya tendrán esa credibilidad para que otros piquen.

De hecho, los ciberdelincuentes saben que si un trabajador recibe la orden para hacer compras o transferencias con la voz de su superior, siempre es más fácil que se lo crea. Se está investigando algunos casos en los que han llamado por teléfono a directivos de empresas y les han suplantado la voz, y, con ella en su poder, el daño puede ser terrible: desde cometer estafas, vender productos en su nombre..., hasta atacar a su reputación; depende de lo que quieran conseguir y de hasta dónde llegue la imaginación de los malos.

10) ¿Crees que se necesita más cooperación entre agencias de seguridad para evitar ciberataques?

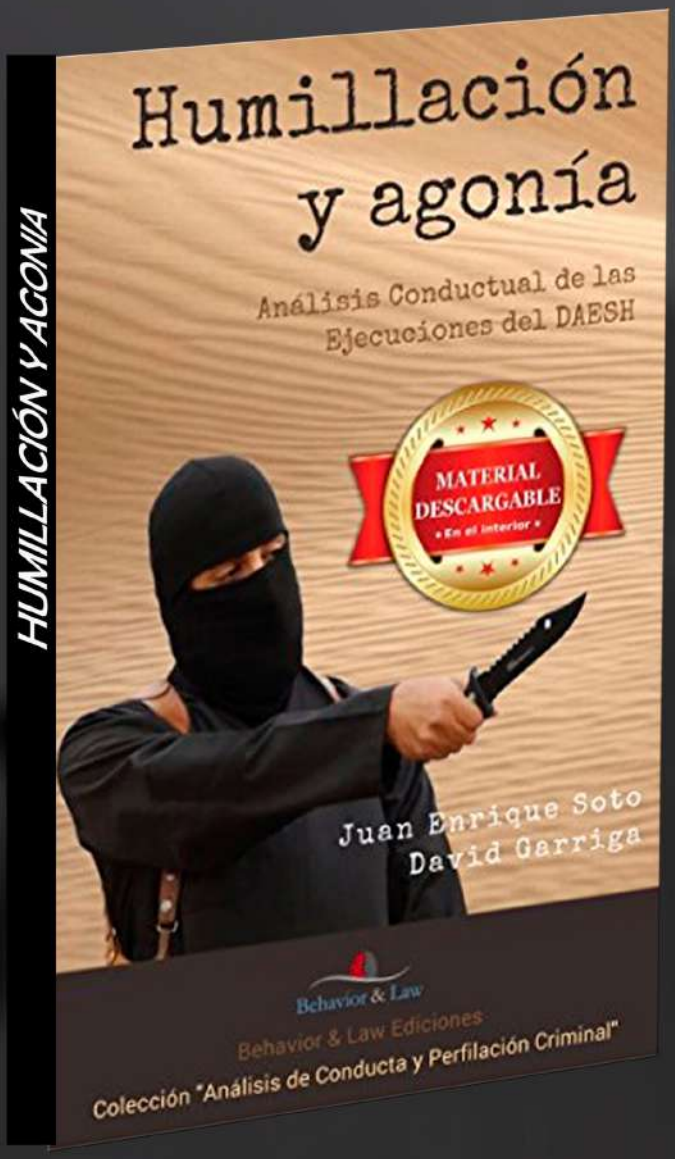
Creo que sobre todo las compañías de tecnología privadas deben colaborar, pero abogó porque las agencias puedan tener acceso a los datos de los potenciales sospechosos de ataques cibernéticos. Por ejemplo hay diferentes tipos de infraestructuras que se dan y se repiten Antes de un ataque y son detectables por los propietarios de dichos servicios.

Si fuésemos capaces de trabajar de forma conjunta mediante IA, y se estableciesen filtros con alertas, muy probablemente seríamos capaces de poder conseguir reducir el tiempo de exposición de un ataque a su audiencia.

Despacho onBranding

Humillación y agonía

Juan E. Soto
David Garriga



Este interesante libro profundiza en el Análisis Conductual de los vídeos que en los últimos años DAESH ha hecho públicos y en los que se muestran algunas ejecuciones de sus rehenes

Behavior & Law

CRIMINOLOGÍA

WWW.ALGHURABA.ORG

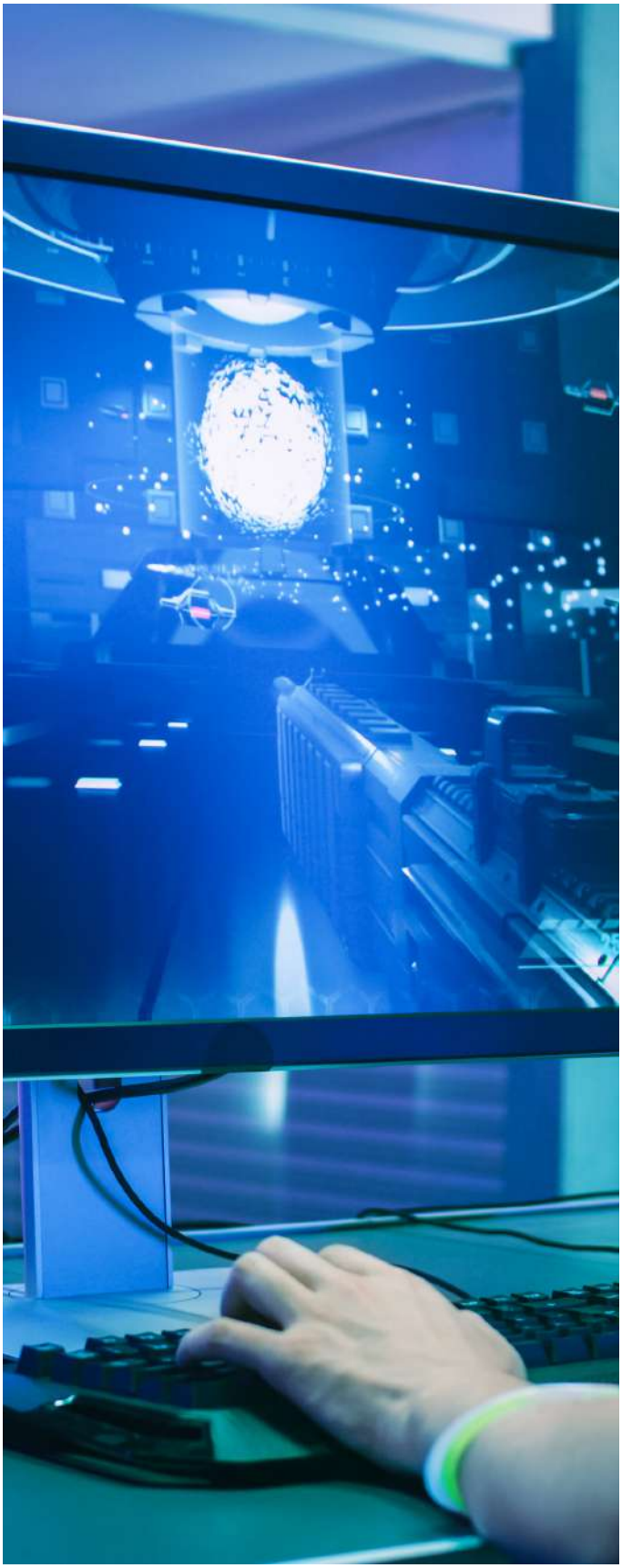
DE LAS PANTALLAS A LA REALIDAD

CAPTACIÓN YIHADISTA A TRAVÉS DE VIDOEJUEGOS

Kristina Tserkovnyuk.
Graduada en el grado de Criminología y Seguridad de la Universidad de Cádiz.
Cursando prácticas universitarias en CISEG

Los grupos terroristas se van adaptando cada vez más rápido a los tiempos que corren y por ende a las nuevas tecnologías. Con la creación del ciberespacio aparecen nuevas formas de comunicación como son las redes sociales o los videojuegos en línea, en donde se permite el contacto entre personas de diferentes partes del mundo, haciendo así más fácil la socialización. Grupos como Daesh utilizan este fenómeno emergente a su favor, ya que por medio de internet es más fácil la difusión de contenido y la captación de nuevos integrantes de una manera más rápida y sin la necesidad de correr peligro.

Con el paso de los años los videojuegos han ido adquiriendo más realismo a la vez que popularidad, sumando así nuevos seguidores cada vez más jóvenes. Nos podemos encontrar un gran número de juegos en la red, de entre todos destacan los bélicos, como es el ejemplo de "Call of Duty". En estos videojuegos nos encontramos situaciones violentas en las que la perspectiva desde la que se juega es la propia, es decir, da la sensación de que el jugador está sujetando el arma. Jugar a estos videojuegos se puede considerar un factor de riesgo debido a que el jugador no presenta consecuencias al matar a los personajes ni se observa la verdadera repercusión de la violencia sobre las víctimas, de esta manera aprenden a inhibir la culpabilidad además de deshumanizar a las personas y a ciertos colectivos. A pesar de ser algo ficticio, tiene consecuencias en la vida real y lo pueden llegar a experimentar en situaciones reales, cabe mencionar que la vi-



-olencia es una conducta aprendida, por lo tanto, estos videojuegos pueden ser uno de los impulsores a futuras conductas violentas.

Los videojuegos bélicos tienen multitud de posturas en contra, como es el caso de Pötzch (2017) quien critica la trivialización que hacen de la guerra y la excesiva violencia gratuita que presentan. Nardone (2017) analiza cómo los videojuegos contribuyen a modificar la percepción de la guerra en los jugadores, al primar lo lúdico por encima de lo realista, minimizando la repercusión de la violencia en las víctimas. Se puede observar como estos videojuegos están presentes en grupos terroristas, desde la apropiación de la estética de los mismos para la creación de sus videos y propaganda hasta utilizarlos como herramientas para la captación, con el objetivo de atraer a un público cada vez más joven. Además, estos grupos también han optado por la creación de videojuegos para el adiestramiento de sus soldados.

Cuando hablamos de captación yihadista no nos encontramos con un perfil específico, ya que todo el mundo puede ser radicalizado si se encuentra en un entorno con unas circunstancias específicas, es decir, con factores de riesgo tanto ambientales como personales. Aunque no existe un único perfil, la mayoría de personas radicalizadas son hombres y la edad media es de 31 años, una media que cada vez desciende más. Cuando hablamos del género masculino, las motivaciones que les lleva a unirse a la causa yihadista son mayoritariamente ideológicas y utilitarias, siendo estas la parte más bélica de la motivación. Si se analiza el perfil de los jugadores de los videojuegos violentos observamos que predomina el género masculino, además de ser los adolescentes los principales usuarios.

Es por ello que en los videojuegos los grupos terroristas encuentran un entorno idóneo para la captación. Los jugadores son sujetos jóvenes puestos en contacto con conductas violentas y en espacios bélicos, sin importar que estos hayan sido ficticios. Además, al ser juegos en línea permiten la conversación entre captadores y usuarios. En un

inicio estas conversaciones no se quedaban guardadas debido al diseño del juego, dificultando así su seguimiento por los servicios de inteligencia y haciendo más sencilla y segura la función del captador. Una vez que el sujeto es radicalizado se le suele enviar a zona de combate, es ahí donde estos videojuegos consiguen traspasar las pantallas y convertirse en una realidad. La muerte deja de ser un juego y los daños hacia las víctimas se vuelven irreversibles.

A pesar de que un gran número de videojuegos de estas características han ido tomando medidas para evitar la captación yihadista a través de sus plataformas, como es la sustitución de mensajes autoeliminados por autoguardados, aún queda un largo camino para que estas plataformas sean seguras. Desde un aporte criminológico se traen algunas propuestas para prevenir la realización de esta conducta.

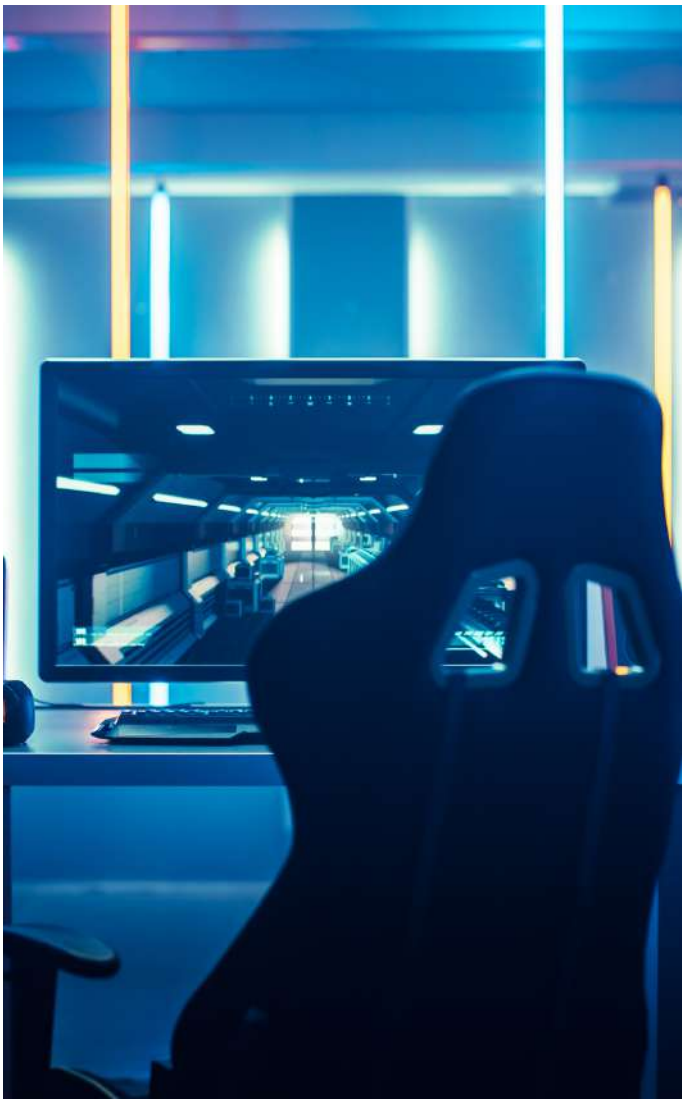
Centrándonos en la estética, contenido y características de los videojuegos, nos encontramos ante un espacio violento en el que los jugadores no se paran a reflexionar los motivos por los cuales matan a los enemigos, además de legitimar este tipo de acciones. Es por ello que estos videojuegos deberían de modificar su contenido para hacerlos más reflexivo y realista, que se observen las consecuencias para el agresor y para la víctima en la partida, también se debería de permitir otras opciones para ganar, no únicamente la de matar, dando así al jugador la oportunidad de decidir. Además de ello poner un límite de edad, ya que los sujetos más jóvenes tienen más facilidad de sufrir una desconexión moral, aprovechando también su facilidad de aprendizaje recurrimos a la educación como medida para evitar la captación a través de videojuegos. Estos juegos violentos, en su mayoría bélicos, tienen un trasfondo histórico y cultural. Utilizándose de una manera correctas pueden ser un método de enseñanza, si los usuarios son conscientes de ello y conocen la historia será más difícil la radicalización de los mismos, ya que el discurso de los captadores se pondrá en duda y perderá sentido.

Como conclusión observamos como los videojuegos bélicos son un recurso presente en los grupos terroristas y como su utilización facilita la tarea de los mismos, no únicamente baja-ndo el factor de riesgo de la captación, si no también preparando a sus jugadores a vivir contextos de violencia. La estética y dinámica de estos juegos es lo que los hace peligros por lo que se tendrían que tomar medidas para que estas plataformas fueran más seguras.

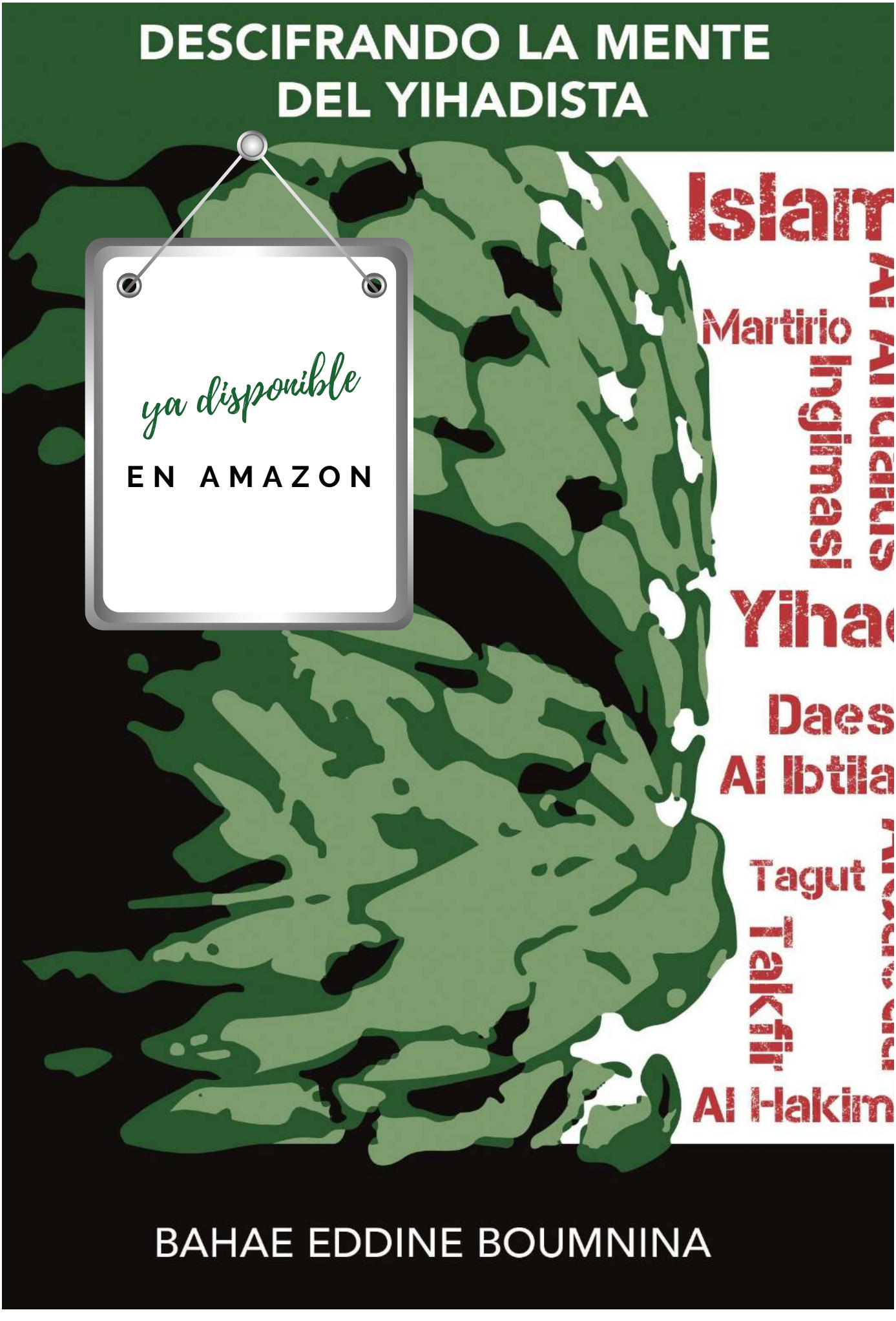
REFERENCIAS

Del Moral Pérez, M. E., y González, C. R. (2021). Revisión sistemática de investigaciones sobre videojuegos bélicos (2010-2020). *Revista Humanidades,* (42), 205-228.

Vázquez, A. G. (2019). *La banalización de la guerra en los videojuegos bélicos* (Tesis doctoral, Universidad de Salamanca).



DESCIFRANDO LA MENTE DEL YIHADISTA

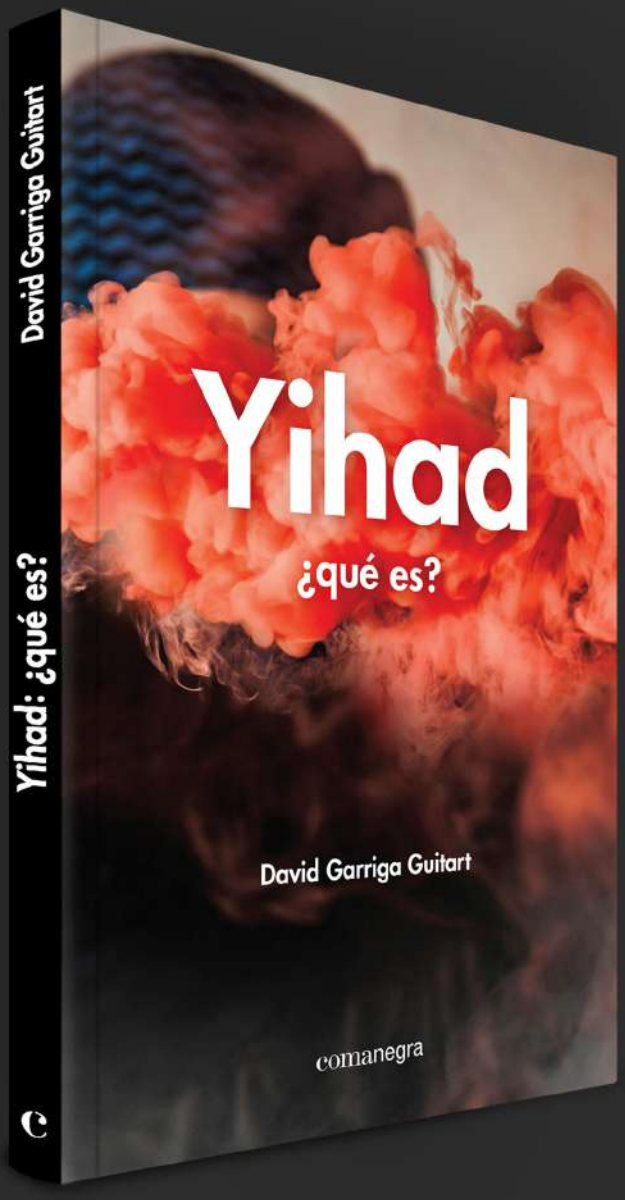


BAHAE EDDINE BOUMNINA

YIHAD, ¿QUÉ ES?

David Garriga Guitart

UNA GUÍA PARA ENTENDER QUÉ ES EL YIHADISMO.



cómpralo con un 5% de descuento en:
www.comanegra.com

*Código de descuento: YHD-17

comanegra

TRIBUNA DE OPINIÓN

WWW.ALGHURABA.ORG

EL PAPEL DE LA CRIMINOLOGÍA

EN EL TRATAMIENTO DE MENORES

Rocío Garví García.
Criminóloga. Intervención con personas infractoras. Valoración del riesgo del delito.

El pasado 5 de junio de 2021 se publicó la Ley Orgánica 8/2021, de 4 de junio, de protección integral a la infancia y la adolescencia frente a la violencia, la cual responde a la necesidad de introducir en nuestro ordenamiento jurídico los compromisos internacionales asumidos por España, integrando a su vez distintos ámbitos de actuación: el familiar, el educativo, el sanitario, los servicios sociales, las nuevas tecnologías, el deporte y el ocio y las Fuerzas y Cuerpos de Seguridad. Dicha Ley interviene principalmente desde tres ejes fundamentales: la sensibilización, la prevención y la detección precoz de la violencia hacia personas menores y adolescentes. Por lo que, atendiendo a estas tres actuaciones principales, no cabe duda de que la figura del criminólogo de-

-bería estar presente. Pero ¿qué funciones específicas podríamos realizar en el marco de esta Ley?

En primer lugar, con respecto a la sensibilización, a la hora de elaborar campañas y acciones concretas destinadas a proporcionar información y concienciar a la sociedad sobre esta problemática, la criminología es esencial debido a que es la ciencia que estudia y trabaja con los diferentes factores de riesgo y protección y su influencia según la etapa vital en la que se encuentre la persona menor o adolescente. Además, disponemos de conocimientos sobre las diferentes tipologías delictivas y su respectivo tratamiento, pudiendo pues, ayudar en la elaboración de campañas más específicas, generando un

impacto más directo. Por lo que el enfoque criminológico en estas acciones se asume de forma indispensable.

En cuanto a la siguiente actuación, dirigida a la prevención de la violencia, podría considerarse el eje fundamental de la ciencia criminológica, pudiendo crear junto a otros profesionales del ámbito social, jurídico y psicológicos planes y programas de prevención primaria, secundaria y terciaria. En referencia a los programas de prevención primaria, es decir, aquellos dirigidos a la población general, se realizarían tareas de concienciación, proporcionando información sobre dicha problemática o fomentando buenas prácticas y trato hacia los y las menores y adolescentes. Seguidamente, a través de los programas de prevención secundaria, enfocados a grupos de riesgo o personas vulnerables, se intentaría reducir o mitigar las diferentes situaciones de desprotección y otros factores de riesgo que pudiesen verse implicados. Finalmente, los programas de prevención terciaria estarían encaminados a proporcionar herramientas de ayuda jurídica, social, psicológica y sanitaria a los niños, niñas y adolescentes que han sido víctimas de cualquier tipo de violencia en cualquiera de los ámbitos anteriormente mencionados, basándonos en las necesidades y características específicas de cada persona tratada.

La tercera línea de acción es la encaminada a la detección precoz de las distintas situaciones de violencia por parte de los profesionales que mantienen contacto habitual con las personas menores y adolescentes. Aunque los criminólogos y criminólogas, debido a nuestra formación interdisciplinar, pudiésemos ser capaces de detectar las sutiles señales de violencia, la realidad que hoy asumimos es que, generalmente, no somos partícipes en las actuaciones llevadas a cabo en centros escolares, servicios sociales o de protección. Es por esto por lo que, una de las tareas fundamentales en las que podríamos participar es en la formación de los profesionales que actualmente sí tratan directamente con infantes y adolescentes, ya que esto podría aumentar la eficacia de la detección de las necesidades de las personas tratadas antes, durante y después de darse los casos de violencia que conciernen en esta Ley.

Como se puede observar, la criminología es una ciencia fundamental que debe ser tenida en cuenta para la realización de buenas prácticas en el marco de dicha Ley. Asimismo, me gustaría comentar algunas funciones específicas que los criminólogos/as podríamos llevar a cabo en los distintos ámbitos de intervención.

En cuanto al ámbito familiar y de servicios sociales, el criminólogo, junto a otros profesionales, podría llevar a cabo el análisis de la situación familiar para poder identificar las necesidades concretas, limitar los objetivos de intervención y las medidas a aplicar; participar en los gabinetes psicosociales de los juzgados y servicios sociales para sugerir medidas penales o de protección del menor, utilizando instrumentos de valoración y gestión del riesgo en las situaciones que se requieran; así como, evaluar las necesidades de las personas infantes o adolescentes en los recursos especializados de atención y protección, detectando posibles casos de violencia de género, intrafamiliar o cualquier otro tipo para su posible derivación a otros servicios de atención especializada.

Seguidamente, me gustaría dar especial atención al ámbito educativo, ya que la Ley mencionada prevé, además de la regulación de protocolos de actuación ante los distintos tipos de violencia, la creación de la figura del Coordinador/a de bienestar y protección. Algunas de las funciones que podríamos llevar a cabo son: promover y coordinar planes de formación sobre prevención, detección precoz y protección a los y las profesionales de los centros educativos, el alumnado y las familias, detectar las posibles situaciones de violencia, fomentar la resolución alternativa de conflictos y el respeto entre el alumnado para promocionar la inclusión y la diversidad, entre otras. ¿Y quién mejor que un criminólogo/a para realizar estas funciones? Formados en las tres líneas de prevención, en mediación, en la identificación y gestión de necesidades criminógenas, en la intervención con víctimas y victimarios, y mucho más. Es por ello por lo que, cuando la presente Ley indica en diversas ocasiones que se contará con la participación de “profesionales de los diferentes sectores implicados en la prevención, detección precoz, protección y reparación de la violencia sobre niños, niñas y adolescentes”

(p.27) debemos pensar que la figura de los y las criminólogas está incluida.

Para finalizar este artículo, me gustaría invitar a reflexionar a los y las profesionales que puedan estar leyendo. Aunque todavía quede mucho camino por recorrer desde el ámbito profesional de la criminología, actualmente empresas y entidades del tercer sector empiezan a ver la necesidad de contratarnos desde distintos ámbitos de actuación. Por esto, debemos seguir esforzándonos desde las universidades, colegios profesionales, asociaciones de estudiantes y demás, en la visibilización de la criminología y en la desmitificación de la imagen fantasiosa y cinéfila creada alrededor de nuestra figura, proporcionando información tanto a la sociedad en general, como a los propios criminólogos/as.

HERRAMIENTAS

WWW.ALGHURABA.ORG

LOS OJOS SON EL ESPEJO DEL ALMA

¿SEGUROS?

Marc Fornós.

Vicepresidente de CISEG. Analista de inteligencia. Especilista en OSINT.

Este mes presentamos una aplicación que algunos les pondrá los pelos de punta, otros abrirán los ojos como platos y puede que algunos les despierte asombro y curiosidad, esta vez presentamos la creación de METAHUMANOS.

Una de las productoras más famosas del mundo por su apuesta de juegos en línea, EPIC GAMES, ahora ha incorporado esta aplicación de creación de metahumanos, en que podremos mediante una figura inicial ir modelándola y crear el metahumano hacia donde nosotros queramos, desde obtener una figura bien parecida a nosotros a poder realizar alguien totalmente anónimo de la nada.

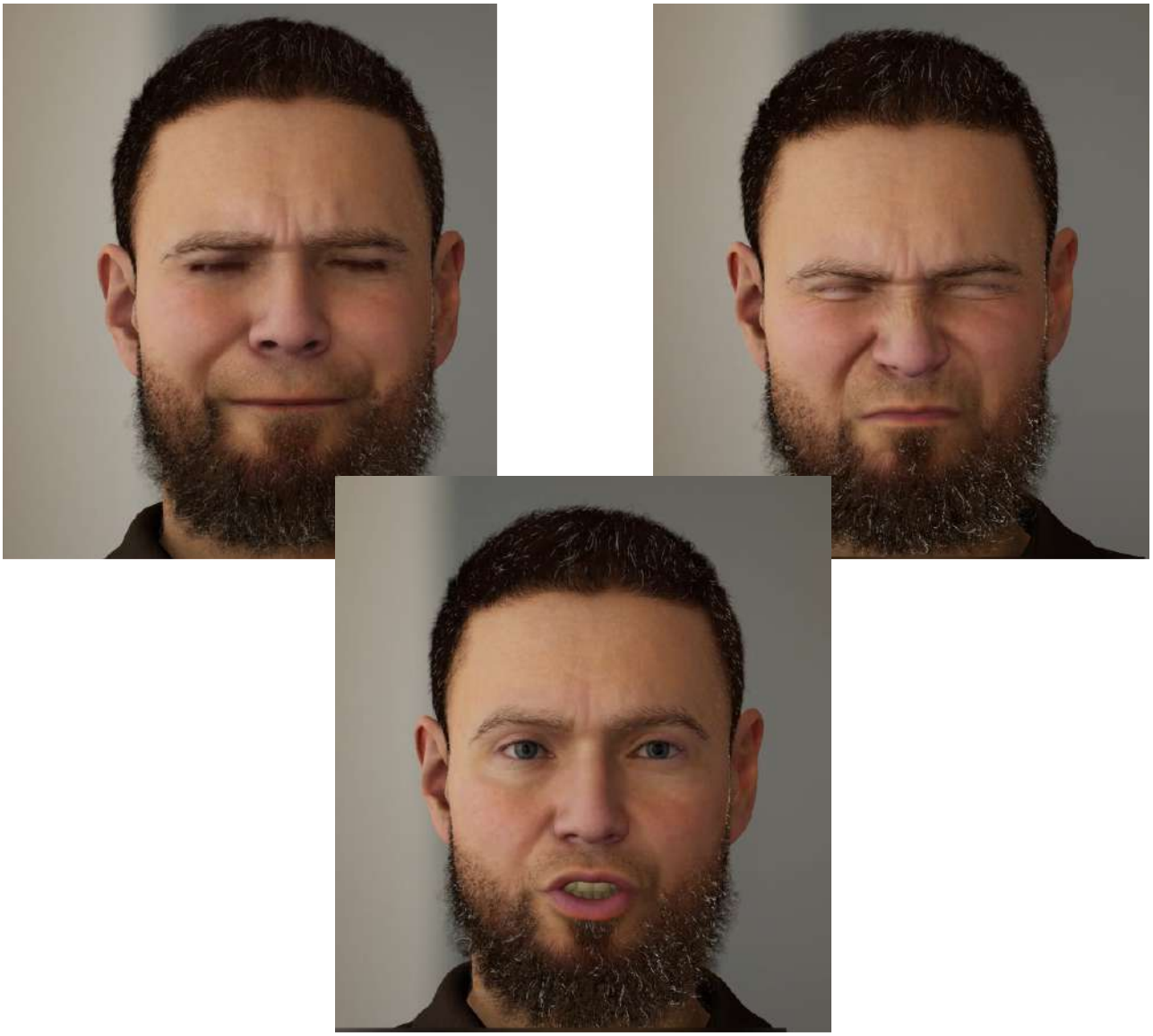
¿Y que son los metahumanos? Son humanos digitales o más bien por decirlo mejor, avatares digitales con apariencia humana realista, y no solo esa apariencia fotográfica que estamos más acostumbrados a encontrarnos en el mundo de la ciber-inteligencia, sino que sé acompañan de gestos, movimientos, marcas del paso del tiempo, emociones, incluso rasgos étnicos que le podemos dar a nuestro metahumano, incluso podremos darle vida en stream haciendo que hable por nosotros con una simple app sincronizada.

Metahuman creator nos brinda la capacidad de ir modificando la apariencia de nuestra "base de metahumano" que queramos escoger, hasta alcanzar la imagen que queremos transmitir o mostrar a nuestro público, realizando cambio a cambio hasta conseguir el aspecto del ideal. La aplicación nos brinda la posibilidad de escoger entre varios modelos ya creados e ir modificándolos en función nuestras preferencias.

En el mundo de la inteligencia y ciber-inteligencia hemos podido encontrar muchos avatares digitales que no existían como los que se producen con algunas aplicaciones de IA para crear esos avatares desestabilizadores o encaminados a realizar "haterismos" de naciones o personas, pero que al ojo del experto ya estábamos acostumbrados a detectar o habíamos realizado ese training visual para poder detectarlos en sitios como "which face is real", donde podemos aprender y obtener cierta habilidad en la detección de esas cuentas fake en forma de BOT de manera muy visual, y nos ayudaba también descubrir esas cuentas que muestran un perfil falso por parte de un posible hacker que quiera realizar esa ingeniería social para obtener información sobre nosotros.

Pero con Metahuman esta fase ha pasado a un 2.0 y más complicado, ya que permite a nuestro personaje darle mucho más realismo en su historia, y darle vida en sus rasgos raciales, envejecimiento, mirada, boca, dientes, podremos hacerle hablar, podremos vestirlo, llevarlo donde queramos, como si fuéramos nosotros mismos visitando por ejemplo un típico rascacielos de Manhatan. Con permiso de una persona muy cercana a mí, le creé un hermano pequeño con rasgos similares a los suyos. En la fase inicial de creación me sentí como una nueva deidad capaz de crear vida, y en este caso lo estaba haciendo, daba vida a un META-HUMANO. Para crear a mi metahumano jugué con la apariencia de fotos antiguas de mí amigo, no siendo la actual sino la de hace unos años, pensé que usando la actual sería algo tenebroso, así que escogí un personaje "tipo", y empecé con la magia del creador de metahumanos. Inicié la fase de modificaciones básicas de mi avatar hasta llevarlo a una semejanza importante de sus rasgos. Me impresiono la cantidad de detalles que podemos definir desde color del esmalte de los dientes, color de la dentina, o el color de las encías, así como algunas posiciones de los dientes, orejas, mentón, ojos...

Una de las cosas a subrayar es sobre todo, una vez vamos creando nuestro metahumano podemos ir viendo, lo realístico del personaje, como se mueve, como se refleja en él esas emociones tan nuestras y que da el realismo humano, e incluso hacerlo hablar.



La verdad que esta aplicación me fascinó y empecé a pensar en las aplicaciones que le podríamos dar desde el mundo de la inteligencia y la seguridad, y siendo una aplicación con estas características la verdad que su aplicabilidad y usabilidad son muchas. ¿por qué no crear retratos robot realmente realistas? ¿O incluso llegar a realizar cambios de aspecto para ser más localizable una persona que está en búsqueda? Y un sinfín de usabilidades que se le va a ocurrir al lector y que se me ocurrieron a mí cuando escribí este artículo, y que permanecerá en el secretismo de todo analista de inteligencia.

La tecnología avanza y los meta-humanos ya llegaron a nuestro mundo, ¿qué será lo siguiente?

AGENDA

¿Quieres promocionar tu próximo evento? Contacta con alghuraba@intelciseg.com

WWW.INTELCISEG.ORG

SIMPOSIUM CRIMEN ORGANIZADO TRANSNACIONAL

Organiza: Colegio Internacional de Investigadores Forenses y #CISEG

✏ 4 y 5 setiembre 2021

** 50% descuento miembros CISEG / IAFI**
** inscritos 1 año membresía gratis CISEG**

✏ Formato de registro aquí

CURSO UNIVERSITARIO

SEGURIDAD, TERRORISMO Y CONTRA-TERRORISMO

eduka formación · Cátedra Proyecto Eduka · Universidad Nebrija · Campus para la Seguridad y Defensa · CISEG · E3A

HAZ CLICK PARA MÁS INFORMACIÓN SOBRE EL CURSO

CURSO UNIVERSITARIO

SANITARIO DE COMBATE EN OPERACIONES

eduka formación · Cátedra Proyecto Eduka · Universidad Nebrija · Campus para la Seguridad y Defensa · E3A

Hemeroteca

Todos los números de
Al-Ghurabá a un golpe de click

AL-GHURABÁ

COLABORADORES







MÁS DETALLES EN

WWW.ALGHURABA.ORG