Nuevas tecnologías del entretenimiento como método formativo en el ámbito del terrorismo

Trabajo Final de Grado

Grado en Seguridad

Universidad de Barcelona – Instituto de Seguridad Pública de Cataluña

Adrián Cantalejo Gámez

Tutor: Jordi Graner Agust

Curso 2022 - 2023

ÍNDICE

1. Introducción y motivación de la investigación……. 1

1.1. Marco teórico……. 3
1.2. Objetivo y pregunta de investigación…… 5
1.3. Metodología de investigación……. 5

BLOQUE I. Cuestiones básicas sobre las nuevas tendencias en el ámbito del terrorismo: videojuegos, radicalización y actores individuales……... 7

2. Videojuegos: ¿factor causal de la violencia?..... 7

3. Videojuegos como factor de atracción a la radicalización violenta…… 9

4. El terrorista individual…… 15

BLOQUE II. Nuevas tecnologías del entretenimiento y potencial formativo en el ámbito del terrorismo……... 20

5. *Serious games*, simuladores y realidad virtual……... 20

5.1. Serious games "básicos"..... 22
5.2. Simuladores avanzados…… 25
5.3. Realidad virtual……... 27

6. Necesidades formativas del terrorismo…… 31

6.1. Fabricación de explosivos……. 34
6.2. Uso de armas de fuego……. 35
6.3. Ejecución de un asalto…….. 37
6.4. Asesinatos……... 40
6.5. *"Ultimate Mowing Machine"*..... 41
6.6. Empleo de drones como arma terrorista…… 41
6.7. Ciberterrorismo……... 42

6.8. Estrategias para evitar la detección…… 44
6.9. Obtención de información y espionaje…… 47
6.10. *Counter Interrogation Tactics*…… 48

7. Escenario futuro: Videojuegos formativos de contenido terrorista…….. 50

7.1. Fabricación de explosivos…… 50
7.2. Uso de armas de fuego…… 52
7.3. Ejecución de un asalto…….. 53
7.4. Asesinatos……... 54
7.5. *"Ultimate Mowing Machine"*..... 56
7.6. Empleo de drones como arma terrorista…… 56
7.7. Ciberterrorismo……... 57
7.8. Estrategias para evitar la detección…… 58
7.9. Obtención de información y espionaje…… 60
7.10. *Counter Interrogation Tactics*…… 61

8. Conclusiones……... 63

Bibliografía…… 68

1. Introducción y motivación de la investigación

Los actos terroristas han sido, desde hace décadas, motivo de atención mediática y popular. Sin embargo, a pesar de lo "llamativo" que resulta, el terrorismo es un fenómeno complejo. Esto se da especialmente por el hecho de que se encuentra en constante evolución. Los grupos terroristas se adaptan a la sociedad en la que operan para tener más posibilidades de alcanzar su objetivo. En este sentido, en la actualidad destacan dos nuevas tendencias de cambio respecto a métodos de actuación previos.

Por una parte, los Estados desarrollados, especialmente en Occidente, poseen fuerzas y cuerpos de seguridad, así como agencias de inteligencia, con el poder necesario para dificultar enormemente el desarrollo del terrorismo colectivo, pese a que este no ha dejado de ser una amenaza. Es por ello que en los últimos años se ha extendido la práctica del terrorismo individual, la cual implica la comisión de atentados por parte de actores individuales independientes de cualquier estructura jerárquica. Esto puede demostrarse a través del estudio de estadísticas oficiales[1] y del análisis de discursos propagandísticos de diversos grupos terroristas. En 2014, Abu Mohammad al-Adnani, ex-líder de Estado Islámico, declaró en un mensaje a sus seguidores lo siguiente:

> *If you can kill a disbelieving American or European – especially the spiteful and filthy French – or an Australian, or a Canadian, or any other disbeliever from the disbelievers waging war, including the citizens of the countries that entered into a coalition against the Islamic State, then rely upon Allah, and kill him in any manner or way however it may be [...] Do not ask for anyone's advice and do not seek anyone's verdict. Kill the disbeliever whether he is civilian or military, for they have the same ruling. Both of them are disbelievers.* (Davidson, 2014)

La orden de no buscar consejo o veredicto externo indica una transición a un terrorismo más alejado de lo que tradicionalmente se ha conocido como una actividad criminal de tipo "social". Esta orientación no es exclusiva del terrorismo yihadista, como puede verse en la "Declaración Europea de Independencia" de Anders Breivik:

[1] El Observatorio Internacional de Estudios sobre Terrorismo (OIET) presenta anualmente un resumen sobre el terrorismo yihadista. En el documento de 2021, se hace un análisis de 35 atentados ocurridos en Europa Occidental entre 2018 y 2021 (p. 56). El 91% de estos atentados fueron protagonizados por un solo individuo.

> Una de las grandes fortalezas de nuestros enemigos, los marxistas culturales de Europa y sus regímenes multiculturalistas son sus vastos recursos y sus capacidades avanzadas de investigación forense. [...] Ellos son superiores en casi todos los aspectos. Pero todo monstruo de siete cabezas tiene un talón de Aquiles. El talón de Aquiles es su vulnerabilidad frente a las células individuales. (Breivik, 2011)

El terrorismo individual presenta ventajas en lo relativo a su detección, la cual se ve dificultada por la ausencia de lazos formales con otros miembros, lo que además genera confusión en los servicios de inteligencia. Sin embargo, los atentados llevados a cabo por actores solitarios suelen tener una naturaleza demasiado simple.[2] Esto se debe a la incapacidad operativa o al *amateurismo* común en el terrorista individual, lo que muchas veces le limita a la hora de seleccionar objetivos o le hace fracasar.

La segunda tendencia a la que se hacía referencia al principio es el uso que hace el terrorismo de las nuevas tecnologías. Es ampliamente conocido el hecho de que los grupos terroristas, especialmente los de naturaleza yihadista, han explotado al máximo las capacidades legítimas y no legítimas que ofrecen los avances tecnológicos para su causa, en particular Internet y las redes sociales. El factor *online* ha facilitado enormemente la difusión de propaganda, la planificación, la instrucción, la coordinación y la financiación del terrorismo, permitiendo que estas actividades tengan una extensión global y, por el contrario, dificultando su persecución por parte de los actores encargados de la seguridad. En el marco de las relaciones entre nuevas tecnologías y grupos terroristas empieza a destacar el papel que tienen los videojuegos y las tecnologías del entretenimiento. La *gamification* o ludificación ofrece ventajas únicas que han sido detectadas por numerosos actores, por supuesto, aquí se incluyen los terroristas, que no han descartado aprovechar el medio. Sin embargo, tal y como se verá en el apartado siguiente, el uso actual de los videojuegos por parte de los terroristas es limitado y básico, pero esto es susceptible de cambiar progresivamente.

Es en este último tema donde se centra la presente investigación. Comprender cómo los videojuegos son y serán utilizados por los terroristas es de especial interés para las fuerzas y cuerpos de seguridad, teniendo en cuenta de que se trata de una innovación -táctica- que mejora las capacidades operativas ya existentes de estos actores (Dolnik, 2007, como se

[2] Toboso (2016) ofrece una descripción de diferentes atentados cometidos por terroristas individuales, se puede observar que estos se limitan mayormente a ataques con armas blancas y que algunos no producen víctimas.

citó en Toboso, 2019). Arrojar luz sobre tal innovación antes incluso de que comience a consolidarse ofrecerá una posición ventajosa en la lucha contra el terrorismo. El hecho de que la Estrategia Nacional contra el terrorismo esté siendo revisada para incluir el estudio de los videojuegos como factor de atracción de la radicalización violenta es un indicador del creciente interés en la cuestión (Toboso, M, comunicación personal, 23 de noviembre de 2022). Pero aún más preocupante resulta la posible relación futura entre las dos tendencias presentadas, especialmente por su alta probabilidad. En la actualidad, los terroristas son individuos que, paradójicamente, se ven influenciados por ciertos valores de la sociedad a la que atacan. En el caso de la sociedad occidental, esta se caracteriza por el individualismo y la digitalización. Esto ha derivado en el aumento de casos de terroristas individuales cuya radicalización se produce a través de las nuevas tecnologías. Por lo tanto, resulta necesario plantear cómo podrían afectar los videojuegos de contenido extremista a los terroristas individuales y, sobre todo, si podrían ser de ayuda para acabar o reducir con su falta de habilidades a la hora de cometer atentados.

1.1. Marco teórico

El uso de las tecnologías por parte de grupos terroristas ha sido ampliamente estudiado desde distintos enfoques, mientras tanto, el análisis del uso que hacen los terroristas de las tecnologías del entretenimiento se ha centrado en su capacidad propagandística. Selepak (2010) examina 28 videojuegos incluidos en la sección de entretenimiento de múltiples sitios web y comprueba que su contenido, desde los enemigos/ adversarios u objetivos hasta el personaje controlado difunden el mensaje de diferentes grupos ultraderechistas. Lakomy (2019) ofrece algunos ejemplos de videojuegos desarrollados -o modificados- por grupos yihadistas desde el inicio de la guerra contra el terror tras el 9/11, como *Special Force* de Hezbolá, *Quest for Bush* de Al-Qaeda o, recientemente, *Huroof* de Estado Islámico. Aunque se trata de videojuegos primitivos el autor explica que la capacidad de interacción ofrecida, la satisfacción obtenida al jugarlos -lo que puede motivar a la repetición- y la relativa facilidad para acceder a ellos son grandes ventajas respecto a otros medios propagandísticos, como artículos de revistas o *fatwas* de líderes yihadistas, los cuales son menos atractivos para las generaciones jóvenes. Por su parte, Schlegel (2020a) explica cómo el Estado Islámico ha hecho referencias a videojuegos populares en la cultura occidental para que pasen a formar parte de su propia “marca” -que se conoce como *jihad cool*- y así tener mayor capacidad de radicalización, desde imágenes o videos con una perspectiva en primera persona al estilo de los populares videojuegos FPS hasta frases citando a *Call of Duty*. Rob van Roy y Zaman (2019) explican que la *gamification*, entendida como la utilización de elementos propios de los videojuegos en diferentes ámbitos, es un

método ideal para satisfacer tres necesidades psicológicas básicas según la teoría de la autodeterminación: percepción de competencia, percepción de autonomía y percepción de conexión o pertenencia. Basándose en esto, Schlegel argumenta que la *gamification* del terrorismo se materializa en tablas de clasificación, tablas de progreso en el proceso de radicalización, rangos, streaming de atentados en vivo, etc. Esto hace que la afiliación al grupo terrorista en cuestión genere placer al usuario.

Sin embargo, la literatura relacionada con el potencial formativo de los videojuegos de contenido terrorista es escasa, lo cual genera intriga ya que en otros ámbitos han sido empleados para tal fin de forma amplia. Esto podría deberse a que el uso de videojuegos con este fin por parte de terroristas no ha salido a la luz, o bien, a qué se trata de una práctica poco frecuente -esta segunda opción es la más probable-. Los casos más destacables son, por una parte, el uso que dieron los autores del 9/11 al simulador de vuelo de Microsoft para planear su ataque (Thurrott, 2001), y por la otra, el de Anders Breivik, que "entrenó" en *Call of Duty* para mejorar su localización de objetivos (Pidd, 2012). Este último ejemplo es cuestionable, ya que se trata de un videojuego comercial con fines no instructivos. En este sentido, la idea más extendida explica que los videojuegos pueden contribuir a la preparación mental del futuro terrorista a través de la desensibilización a la violencia, el desprendimiento moral y la percepción de autoeficacia (Toboso, 2022). Pero no se ha tratado el cómo podrían desarrollar habilidades prácticas o tangibles, como organizar un tiroteo o colocar un explosivo, aunque es una posibilidad que sí ha sido contemplada. Lakomy (2019) establece una interesante relación entre los juegos formativos o *serious games* y la *open source jihad*, concepto utilizado para referirse a los manuales yihadistas que circulan por la red gratuitamente que pretenden desarrollar conocimientos sobre fabricación de bombas, asesinatos, destrucción de edificios y otros atentados (Wiskind, 2016). Dichos manuales son utilizados frecuentemente por terroristas individuales para obtener un mínimo conocimiento antes de ejecutar un atentado.

Gorman (2012) considera a los *serious games* o juegos formativos como una tecnología disruptiva, es decir, se trata de una idea novedosa que a corto plazo no resultará atractiva cuando se introduzca en un ámbito, por lo que no recibirá la suficiente atención o financiación en comparación a los programas de preparación previos. Pero si son gestionados adecuadamente, a largo plazo superarán en efectividad a los mecanismos clásicos. Si aplicamos esta idea a nuestro caso de estudio, se puede deducir que actualmente los grupos terroristas no se han sumado a la tendencia de dar un uso formativo a los videojuegos ya que han priorizado a los métodos tradicionales, lo que explica la escasez de ejemplos. Sin embargo, de la teoría de Gorman también se deriva la posibilidad

de que progresivamente se muestren más receptivos a la adopción de esta tecnología al ver sus resultados en otros ámbitos. La adopción dependerá también de la facilidad para obtener, modificar o crear videojuegos formativos que sirvan a sus intereses, en este sentido, el constante avance a pasos de gigante en la industria asegura que su precio se reducirá progresivamente hasta normalizarse. Por estas razones, no es conveniente descartar el uso de videojuegos con fines formativos por parte del terrorismo.

1.2. Objetivo y pregunta de investigación

Como se ha indicado al principio, la intensificación de la relación entre terrorismo y videojuegos es altamente probable, sin embargo, no se le ha dedicado la suficiente atención en su vertiente instructiva o formativa, a pesar de que es la más peligrosa. Bajo este supuesto, el objetivo de la investigación es comprender las necesidades formativas de los grupos terroristas actuales y determinar cómo podrían ser satisfechas mediante las tecnologías del entretenimiento. Por ello, la pregunta de investigación principal de este trabajo es la siguiente:

- ¿De qué formas podrían ser aprovechados en el futuro (2023-2050) los *serious games* y otras tecnologías del entretenimiento para satisfacer las necesidades formativas del terrorismo, especialmente de los terroristas individuales?

Se ha decidido no poner el foco de atención sobre una tipología de terrorismo en particular ya que de forma generalizada todas están adoptando las mismas tácticas: nuevas tecnologías y terrorismo individual. Sin embargo, los casos expuestos a lo largo de la investigación forman parte del terrorismo yihadista, de extrema derecha o etnonacionalista[3] y esto se debe simplemente a que son las tipologías predominantes actualmente.

1.3. Metodología de investigación

Para responder a la pregunta de investigación se ha optado por emplear, exclusivamente, el método cualitativo, en particular a través del análisis documental. Esta investigación está

[3] Se trata de una tipología creciente que no puede situarse ni en la extrema derecha ni en la izquierda, sino que bebe del fascismo en lo que se refiere al funcionamiento de la sociedad. Pero su característica principal es la defensa de la homogeneidad blanca, considerando como enemigo a todo aquel que la pone en peligro: inmigrantes en países de mayoría blanca y políticos que “toleran” esta inmigración o mezcla racial. Se diferencia de movimientos racistas por el hecho de que dicen “proteger” la diversidad racial o cultural, de forma similar a la lógica de Huntington en su “Choque de civilizaciones”. No abogan por el genocidio de las razas no blancas, sino por la remigración o, como mínimo, por la segregación. Anders Breivik, Brenton Tarrant o Dylann Roof forman parte de esta tipología (Baqués et al., 2022).

dividida en dos bloques principales. El primer bloque se basa en la revisión de documentos centrados en una serie de cuestiones relacionadas con los videojuegos y la violencia, los videojuegos y la radicalización y las características del terrorista individual, cuya comprensión es necesaria antes de profundizar en la materia. El segundo bloque, enfocado en la pregunta de investigación, estudia el estado actual / futuro de las tecnologías del entretenimiento y analiza las necesidades formativas de los grupos terroristas en base a sus manuales obtenidos a través de fuentes abiertas. En la presente investigación no sólo se considerará como tecnología del "entretenimiento" a los videojuegos formativos básicos, sino también a los simuladores y los dispositivos de realidad virtual, por lo que serán contemplados por igual. Finalmente, necesidades y posibilidades formativas serán combinadas para extraer conclusiones y plantear opciones mediante las cuales los videojuegos podrían ser de utilidad para el terrorismo y su actual déficit formativo.

BLOQUE I: Cuestiones básicas sobre las nuevas tendencias en el ámbito del terrorismo: videojuegos, radicalización y actores individuales

2. Videojuegos: ¿factor causal de la violencia?

Una idea subyacente en el uso de videojuegos por parte de grupos terroristas -sea con finalidad propagandística o formativa- es la de cómo estos pueden generar en el jugador comportamientos agresivos y violentos, por ello conviene considerarla brevemente. En realidad, es una idea con defensores y detractores por igual. Si bien la popularización de la industria del videojuego y las plataformas de streaming han logrado que los videojuegos violentos hayan dejado de ser vistos con el tiempo como un fenómeno *underground* -de la misma forma que el género *heavy metal* se ha extendido actualmente cuando era tildado de satánico en sus inicios- el debate sobre su peligrosidad continúa, y este procede especialmente de Estados Unidos a causa del fenómeno de los *school shooters*.

Un estudio llevado a cabo por profesores de la universidad de Villanova, Virginia Tech y la universidad estatal de Pensilvania analizó 204796 artículos de periódico sobre 204 tiroteos masivos -en escuelas y otras localizaciones- cometidos en Estados Unidos entre 1977[4] y 2018. Mediante una búsqueda de palabras clave, se determinó que 6814 de estos artículos incluían la palabra “videojuegos” (Markey et al., 2020). El hallazgo del estudio es fácilmente observable a través de la información ofrecida por distintos artículos sobre los autores de la masacre de Columbine, el tiroteo de Virginia Tech, el de la Escuela Primaria Sandy Hook, el de la Escuela Secundaria de Santa Fe o el de la Escuela en Uvalde. Sus descripciones hacen referencia al consumo -constante- de videojuegos violentos. Los tres primeros casos generaron una mayor controversia, hasta el punto de que medios de comunicación y políticos establecieron una relación causal entre exposición a videojuegos violentos y estas tragedias, pero no han sido los únicos, diversos investigadores reafirmaron este vínculo (Markey et al., 2015).

Por ejemplo, Grossman (1998) considera que los videojuegos enseñan a matar a través de la desensibilización, la generación de estímulos que empujen a una respuesta violenta rápida y un condicionamiento clásico basado en la asociación de violencia y placer. Desde un plano psicológico, Anderson y Dill (2000) trataron de demostrar en base al modelo GAM (*General Aggression Model*) que los videojuegos violentos suponen un input situacional que,

[4] El estudio únicamente incluyó tiroteos masivos a partir de 1977 ya que se consideró que en esta fecha la industria del videojuego disfrutó de un primer estallido en su popularidad (Markey et al., 2020).

a corto plazo, deriva en pensamientos y comportamientos agresivos, mientras que a largo plazo permite el aprendizaje de estructuras de conocimiento relacionadas con la violencia -sesgo de atribución hostil, actitudes positivas frente al uso de la violencia y creencia de que la violencia es una solución efectiva-. Para ello realizaron dos estudios: uno de tipo correlacional orientado a largo plazo y otro de tipo experimental orientado a corto plazo. El primero consistió en un cuestionario autogestionado donde los participantes debían contestar preguntas sobre sus videojuegos favoritos y horas de juego, items medidores de la irritabilidad y de los rasgos de agresión y ciertas preguntas sobre posibles delitos -divididos entre delitos que implicaran agresión y los que no- cometidos el año anterior. Los resultados indicaron una relación positiva entre los conceptos, siendo los participantes que estaban más expuestos a videojuegos violentos los que obtuvieron un mayor índice de agresividad y delincuencia. El segundo estudio requirió que los participantes jugaran durante 15 minutos a un videojuego. Los participantes fueron divididos entre aquellos que experimentaron con un videojuego violento y los que experimentaron con uno no violento. Tras esto, fueron sometidos a una competición ficticia cuyo objetivo era pulsar un botón más rápido que el rival. El perdedor recibiría como castigo un ruido molesto, cuya intensidad y duración sería determinada por el ganador. Los resultados indicaron que los participantes que fueron expuestos a videojuegos violentos seleccionaron una intensidad y duración mayor, lo que se definió operacionalmente como una mayor agresividad.

Aunque las conclusiones de estos investigadores resultan interesantes e incluso guardan relación con nuestro objeto de estudio,[5] no son lo suficientemente fuertes como para demostrar una vinculación directa entre videojuegos y violencia. El problema de los estudios anteriores es la manera en la que definen el comportamiento agresivo (Markey et al., 2015). Por motivos éticos, están limitados a emplear indicadores *soft* para medir la agresividad de una persona -índices de irritabilidad o el someter al otro a un ruido molesto de mayor intensidad y duración- que no son comparables a manifestaciones graves de violencia -homicidios, robos a mano armada, tiroteos masivos o terrorismo-. Pese a esto, generalizan los resultados y los relacionan con tales manifestaciones (Ferguson, 2011). Por esta razón, se han desarrollado nuevas investigaciones con un enfoque más crítico. Esta nueva corriente ha demostrado que, desde 1978 hasta 2011, las ventas de videojuegos y los crímenes registrados en Estados Unidos mantienen una relación inversamente proporcional: en este período la industria del videojuego ha crecido, sin embargo el crímen se ha visto

[5] En especial las afirmaciones de Grossman (1998) sobre la desensibilización, la generación de estímulos que deriven en una respuesta violenta y el condicionamiento clásico. Se trata de factores que serán retomados en los próximos apartados, cuando hablemos del potencial radicalizador y formativo de los videojuegos para el terrorismo.

disminuido[6] (Markey et al., 2015). Otros estudios han afirmado de forma explícita que no existe una relación causal entre exposición a videojuegos violentos y la comisión de actos violentos en la vida real, cuestión distinta es que individuos sometidos a terceros factores que les empujen a la violencia -biológicos, familiares o sociales- tengan una mayor predilección por jugar a este tipo de videojuegos (Rueda et al., 2008; Ferguson, 2011). De hecho, desde hace años la atención está puesta sobre esos terceros factores. En 2004, el servicio secreto y el departamento de educación de Estados Unidos examinaron 37 incidentes de *school shooters* ocurridos entre 1974 y el 2000 y elaboraron un perfil de los autores. Entre sus características se encontraron relaciones sociales inestables o inexistentes, acoso escolar, enfermedades mentales diagnosticadas, pensamientos suicidas, abuso de sustancias, pérdida de un ser querido, fracasos personales, etc.

Esta última conclusión, derivada del estudio de los tiroteos masivos, es trasladable al objeto de esta investigación, el terrorismo. No tiene sentido afirmar que, por ejemplo, la adicción a los videojuegos de Breivik (Berglund, 2012) o Tarrant (Vonow, 2019) los convirtió en individuos violentos y que por ello ejecutaron actos terroristas. Fueron los terceros factores antes mencionados los que les llevaron a hacerlo. Pero dado que el terrorismo es un tipo de violencia política -distinta a la ejercida por los *school shooters*- estos factores no fueron el acoso escolar, las malas relaciones o una enfermedad mental, sino los factores exógenos de radicalización. En este sentido, los videojuegos siguen manteniendo una peligrosa relación indirecta con el terrorismo: tal y como veremos en el siguiente apartado, poseen una serie de elementos que allanan el camino a estos factores y hacen que el jugador sea más receptivo a la narrativa extremista violenta del grupo.

3. Videojuegos como factor de atracción a la radicalización violenta

Antes de estudiar cómo los videojuegos podrían emplearse con fines formativos en el ámbito del terrorismo, es necesario entender su utilidad adoctrinadora. Los grupos terroristas son dependientes de que exista un flujo constante de fieles a su causa. En este sentido, los métodos de radicalización evolucionan progresivamente a medida que avanza la sociedad donde el público objetivo habita. Los largos discursos de líderes yihadistas incitando la destrucción de los infieles occidentales o la participación en reuniones multitudinarias de extrema derecha, si bien siguen siendo focos peligrosos de radicalización, han perdido peso en una sociedad de la impaciencia donde se valora la gratificación inmediata, algo que ofrecen las nuevas tecnologías (Anderer, 2019). La radicalización a

[6] De forma contraria a lo que cabría pensar según las conclusiones anteriores, una mayor exposición a la violencia en los videojuegos no deriva en una oleada de violencia en la vida real.

través de Internet y las redes sociales es una vía ampliamente conocida, sin embargo, la producida a través de videojuegos u otras tecnologías del entretenimiento resulta novedosa y aún no se ha extendido notablemente, pese a sus múltiples ventajas. Este apartado se centra en los videojuegos con contenido propagandístico extremista y en el fenómeno de la ludificación, en cambio, no será abordado el empleo de chats de texto, comunicación por voz y video chat en videojuegos populares -cuyo contenido es legal- para difundir propaganda, reclutar e incluso financiar aprovechando que estos canales suelen estar menos monitorizados (EU Counter-Terrorism Coordinator, 2020). La razón de ello es simple: este tipo de radicalización es más cercana a la que se produce en comunicaciones propias de redes sociales, lo que escapa de esta investigación.

No son escasos los videojuegos modificados por grupos terroristas o creados por ellos mismos. *Special Force* de Hezbolá, *Quest for Bush* de Al-Qaeda o, recientemente, *Huroof* de Estado Islámico. La extrema derecha también ha publicado una gran cantidad de juegos de navegador en sus foros web. La mayor parte no destaca por su portento técnico, de hecho, son videojuegos sumamente básicos e incluso anticuados, pero reflejan la narrativa extremista violenta[7] de sus respectivos grupos y logran expandirla de forma efectiva. Aunque no son un medio infalible, los videojuegos aumentan la predisposición del jugador a exponerse a esta narrativa ya que lo hace al mismo tiempo que participa en una actividad estimulante. Incluso dicha exposición puede tener lugar subconscientemente: la emoción propia de los videojuegos puede difuminar la "resistencia" ante los mensajes ideológicos (Schlegel, 2020a). Además, la popularidad de los videojuegos actualmente es indiscutible. Según un informe de *DFC Intelligence,* el 40% de la población mundial consume videojuegos, es decir, aproximadamente 3100 millones de personas (*Crece El Público Gamer: Un Estudio Revela Sus Ganancias Y Tendencias Esenciales Para Este año*, 2022). Con estas cifras, es natural que los grupos extremistas aspiren a aprovecharse de este fenómeno. Tal y como afirma Pieslak (2017), para atraer a la población a una ideología radical es conveniente cubrirla con un "disfraz" familiar para niños, adolescentes y adultos de la sociedad digital.

El mecanismo más obvio por el cual los videojuegos de contenido extremista facilitan enormemente el proceso de radicalización es a través de la desensibilización a la violencia

[7] La narrativa extremista violenta es una línea argumentativa, basada en principios religiosos, políticos o étnico-nacionalistas, que es legitimada y defendida por los miembros del grupo terrorista. Incluye estos elementos principales (Moyano Pacheco, 2020): identificación de una injusticia o un agravio al grupo y sus ideales, identificación de culpables de la injusticia y de los enemigos del grupo, justificación y promoción de la actuación violenta y, por último, identificación de los beneficios (personales y colectivos) de seguir los principios en los que se basa el grupo.

y, consecuentemente, el desprendimiento moral (Schlegel, 2020b). La desconexión moral permite el "desenganche" respecto a los principios éticos adquiridos por el individuo, la protección frente a sentimientos como la vergüenza y la culpa y evita las auto sanciones o conflictos morales (Bandura, 2002, como se citó en Martínez González et al., 2020). Por supuesto, esto es vital para que las organizaciones extremistas logren incitar a un individuo a cometer un atentado, teniendo en cuenta que la mayoría de terroristas no sufren perturbaciones mentales, sino que en su parecer actúan racionalmente (Toboso, 2019, 35). Los videojuegos logran el desprendimiento moral de tres formas: reinterpretación de la conducta, distorsión de las consecuencias y detrimento de la víctima (Martínez González et al., 2020). La reinterpretación de la conducta se materializa con: una justificación moral de la violencia que la convierta en un medio heroico para alcanzar un propósito superior; una etiquetación eufemística que atenúe la naturaleza del acto violento[8] y la comparación ventajosa, la cual argumenta que la violencia ejercida por el individuo es leve e incluso benigna en comparación con los actos del grupo victimizado.[9] Por otra parte, los videojuegos muestran una representación distorsionada y suavizada de las consecuencias físicas de la violencia en el cuerpo humano o las consecuencias sociales en el colectivo victimizado. Por último, el desprendimiento requiere de la culpabilización y deshumanización de la víctima, lo que elimina la empatía de aquel que ejerce la violencia. Especialmente los videojuegos en primera persona tienden a mostrar un gran número de enemigos en pantalla, esto, complementado con una variedad de métodos para eliminarlos, provoca que dar muerte sea visto como algo rutinario sin importancia, un mero proceso que ha de cumplirse para alcanzar un objetivo. En efecto, se produce una habituación a la violencia (Grizzard et al., 2014). Pero más allá de la habituación, el videojuego está diseñado para que el jugador disfrute de la violencia mediante puntuaciones, premios y efectos visuales o sonoros satisfactorios. Como afirmaba Grossman (1998), esto se trata de un ejemplo de condicionamiento clásico similar al de los perros de Pavlov, donde el jugador asocia el acto de matar con el placer.

Nótese que los videojuegos no son el único medio a través del cual alcanzar el desprendimiento moral. La reinterpretación de la conducta, la distorsión de las consecuencias, el detrimento de la víctima e incluso la difusión de la responsabilidad forman parte de la narrativa extremista violenta, por lo que cualquier proceso de radicalización,

[8] Los adultos reaccionan más agresivamente cuando el ejercicio de la violencia contra otra persona recibe una etiquetación sanitizada o catalogada con palabras "higiénicas" (Bandura, 1990). Por ejemplo, catalogando a las víctimas como objetivos legítimos, a los civiles muertos como daños colaterales o definiendo el acto de matar como neutralización.

[9] Por ejemplo, los grupos yihadistas consideran que los atentados en Occidente no son comparables al gran daño causado por los bombardeos en Oriente Medio por parte de Estados Unidos.

independientemente del medio, debe perseguir esto. Sin embargo, los videojuegos permiten integrar la narrativa extremista violenta directamente en el *gameplay*, por lo que el jugador puede experimentarla y empaparse de esta mientras interactúa con el mundo del juego. Numerosos estudios ya han demostrado la efectividad del aprendizaje activo en comparación con el aprendizaje pasivo (Aupperlee, 2021; Zhang, 2005) en el ámbito educativo, pero es un beneficio también aplicable a la "educación" de individuos radicalizados. El aprendizaje basado en la interactividad mejora el desempeño del estudiante y su nivel de satisfacción. En concreto, el aprendizaje mediante videojuegos facilita la activación de mecanismos cognitivo-emocionales que promueven las reacciones emocionales positivas y la diversión, las cuales aumentan el nivel de atención y la retención memorística respecto al contenido ofrecido, además de motivar al jugador a continuar con el proceso (Schlegel, 2020a). Esto último es especialmente importante teniendo en cuenta que el desprendimiento moral no es un proceso inmediato y total, sino que debe darse progresivamente a través de la repetición (Martínez González et al., 2020).

Precisamente este grado de interactividad hace que los videojuegos sean la mejor vía para aumentar la autoeficacia percibida. A diferencia de otros métodos de radicalización, los videojuegos permiten adentrarse en una narrativa extremista violenta desde un rol protagonista. La cámara en primera persona, los gráficos cada vez más realistas y la capacidad para poder modificar el avatar permite al jugador identificarse con este (Schlegel, 2020b). Desde su punto de vista, el jugador no es un sujeto pasivo que se ve influido por la narrativa o por los actos heroicos en nombre de esta por parte de otros individuos, sino que es el héroe, el foco de atención. Esto mejora su autoeficacia percibida, es decir, la creencia del jugador en su habilidad para poder llevar a cabo las actividades virtuales en el mundo real, incluido el ejercicio de la violencia. Esto no solo le motivará a seguir progresando en la pirámide de la radicalización, un sujeto con el pensamiento (real o no) de que puede llegar a tener éxito a la hora de dañar a otros individuos es mucho más valioso para el grupo terrorista que un sujeto con dudas y miedo.

También es necesario mencionar la relevancia de la ludificación o *gamification* de la radicalización. La ludificación no implica el uso explícito de videojuegos, sino la inclusión de sus elementos comunes o de referencias a juegos populares en la propaganda del grupo extremista. La ludificación con finalidad radicalizadora puede tener dos sentidos: *top-down o bottom-up* (Schlegel, 2020a). La ludificación *top-down* es aquella iniciada por las organizaciones extremistas. Esta puede incluir un sistema de rangos o niveles en foros, un sistema de reputación o insignias virtuales que se obtienen a medida que se progresa en el proceso de radicalización (Hsu, 2011). Estos elementos suponen un *feedback* satisfactorio

para aquellos usuarios competitivos interesados en los logros personales, los cuales se ven incentivados a intensificar su grado de radicalización con tal de aumentar su estatus (Robson et al., 2016). Los elementos ludificadores también pueden atraer a personas interesadas en el ámbito social y la interacción con otros usuarios, produciendo el mismo resultado: una mayor participación en el proceso de radicalización. Por ejemplo, el Movimiento Identitario planificó el lanzamiento de la app *Patriot Peer*, destinada a conectar individuos y a facilitar los contactos dentro del movimiento. La app permitía obtener una mayor puntuación mediante el establecimiento de más conexiones, la asistencia a eventos importantes o la visita a lugares culturalmente importantes para el grupo (Ebner, 2019, como se citó en Schlegel, 2020a). Por lo tanto, la *gamification*, más allá de ser una forma atractiva de extender la ideología en la sociedad moderna, permite satisfacer tres necesidades psicológicas básicas según la teoría de la autodeterminación: percepción de competencia, percepción de autonomía y percepción de conexión o pertenencia a una comunidad (Rob van Roy y Zaman, 2019). La ludificación *bottom-up* es aquella protagonizada por los propios individuos sujetos a un proceso de radicalización o por los propios autores de actos violentos y atentados terroristas, ya sea por su habituación a estos elementos o por la intención de aumentar su popularidad (Schlegel, 2020a). Esto último puede verse a través del streaming en vivo de ciertos atentados, como el cometido por Brenton Tarrant en Christchurch, que filmó sus actos desde una perspectiva similar a la utilizada en los videojuegos en primera persona (Veloso, 2019). Dicho formato es susceptible de fomentar efectos réplica, de hecho, en foros de 8chan se extendió la idea de superar la puntuación de Tarrant, haciendo referencia al número de víctimas que provocó (Evans, 2019), y meses después, en Halle, Stephan Balliet filmó su ataque a una sinagoga también con un formato en primera persona (Val, 2019).

En definitiva, los videojuegos son y serán un arma poderosa para el terrorismo en lo que se refiere a la radicalización por dos grandes motivos. Por una parte, los videojuegos y la ludificación, junto a los videos de rap de letra extremista (Sandberg et al., 2021) o la propaganda de carácter hollywoodense (Zurro, 2017) forman parte de una estrategia destinada a aumentar la popularidad de estos movimientos haciendo una intensa apelación a la cultura de la imagen. En la actualidad la gratificación inmediata y la superficialidad priman sobre la profundidad. Los grupos extremistas han debido adaptarse a ello y han cubierto su mensaje de distintas capas externas que modifican su estética para que sea percibido como *cool* por parte del público objetivo. Esto es especialmente relevante en el caso del yihadismo, dándose una convergencia cultural entre símbolos islamistas y occidentales denominada *jihadi cool* (Sageman, 2008, como se citó en Sandberg et al., 2021). Por otra parte, como se ha mencionado previamente la radicalización es un proceso,

no un fenómeno que se dé inmediatamente. Este se compone de varias fases, desde la simple percepción de una situación injusta hasta la voluntad de cometer un acto terrorista. Existen diferentes modelos que ilustran dichas fases, siendo uno de los más destacables el de Fathali Moghaddam. El autor presenta diferentes plantas a modo de escala, a medida que el individuo asciende por estas su grado de radicalización aumenta (Moghaddam, 2005):

- La primera fase implica la percepción de deprivación, de una situación de injusticia.
- Ciertos individuos ascenderán a la segunda fase y realizarán una búsqueda de soluciones para esta situación.
- Sentimiento de frustración por el fracaso de las acciones y soluciones propuestas. En la tercera fase se produce un desplazamiento de la agresión y los individuos culpan a otros por la situación de injusticia.
- En la cuarta fase, los individuos desarrollan una predisposición a la violencia ejercida contra los culpables de su situación gracias a un desprendimiento moral.
- Los que han ascendido a esta última planta ya se han sumergido en la subcultura extremista en cuestión, ya sea a través de un grupo o individualmente. Se produce una legitimación de los objetivos perseguidos por el movimiento, una creencia de que el fin justifica los medios y un fortalecimiento de una visión dicotómica del mundo. Son los pertenecientes a esta planta los susceptibles de cometer un atentado.

Sin embargo, en la práctica los procesos de radicalización rara vez siguen un orden lineal (Álvarez, 2018), por lo que su estudio se hace verdaderamente complejo. El proceso de radicalización es un camino que lleva a la voluntad de ejercer la violencia. Hasta cierto punto, el individuo puede abandonar y retroceder. Pero al mismo tiempo, puede hacer el recorrido a un ritmo sumamente acelerado, incluso omitiendo escalones del modelo de Moghaddam. Esto dificulta el seguimiento de individuos peligrosos por parte de los servicios de inteligencia (Peña Alonso, 2019) ya que genera un margen de tiempo menor para detectar pruebas, indicadores y señales débiles. Conectando esto con el objeto de la investigación, se puede considerar que los videojuegos de contenido extremista y la ludificación impulsan esta aceleración, principalmente por que sus características -interactividad, percepción de autoeficacia, diversión, socialización, satisfacción- enganchan al jugador y lo someten a una exposición continua de factores exógenos.

4. El terrorista individual

Si bien esta investigación estudia el posible empleo de los videojuegos y las tecnologías del entretenimiento como método formativo en el ámbito del terrorismo en general, incluyendo al terrorismo clásico o colectivo, también conviene centrar la atención en la figura del terrorista individual puesto que es una tendencia o estrategia creciente y muy conectada a las nuevas tecnologías.

El terrorista individual, también conocido coloquialmente como lobo solitario, puede ser definido de diferentes formas. David Garriga Guitart considera que es aquel individuo que siempre actúa en solitario, no pertenece formalmente a ninguna estructura jerárquica o red terrorista, no obedece a las órdenes de un líder y decide por sí mismo sus objetivos, tácticas y recursos (Arias Gil, 2018). El terrorista individual no sólo actúa por su cuenta durante la acción violenta, sino también durante la fase de planificación. Anders Breivik, Brenton Tarrant, Stephan Balliet, Timothy McVeigh, Ayoub el Khazzani, Mohamed Merah o aquí, en España, Yasin Kanza (Peñalosa, 2023)... Son algunos casos de terroristas individuales cuyos actos, fueran más o menos letales, han sido motivo de preocupación por lo impredecibles que resultaron.

El terrorismo individual no es un fenómeno nuevo, sino que se remonta hasta el terrorismo anarquista del siglo XIX. El concepto de propaganda por el hecho desarrollado por diversos ideólogos del movimiento sumado a las apologías directas al terrorismo autónomo e individual[10] provocaron que los actores pertenecientes a esta tipología de terrorismo trabajaran en pequeñas celulas o en solitario. Un buen ejemplo es la Mano Negra serbia, que acabó con la vida del archiduque Francisco Fernando en 1914 y funcionaba en base a células con poca conexión entre sí. Posteriormente, a mediados del siglo XX, la extrema derecha estadounidense rescataría el concepto bajo el nombre de “resistencia sin líderes”. Louis Beam, figura relevante del KKK, afirmó en su artículo *Leaderless Resistance* de 1983 que la forma más efectiva de garantizar el éxito terrorista contra el Gobierno Federal era la no organización. La clásica organización piramidal suponía una amenaza para sus propios miembros ya que por su naturaleza era susceptible de infiltración gubernamental y bastaría con la eliminación de su líder para provocar la desintegración. Beam insiste: para hacer frente a un Estado moderno y desarrollado el esfuerzo ha de realizarse a nivel individual.

[10] Por ejemplo, en 1885, el periódico anarquista *Chicagoer Arbeiter-Zeitung* publicó en un artículo la necesidad de plantearse, antes de llevar a cabo una acción violenta, si realmente era necesario ejecutarla en grupo o si en cambio un único individuo era suficiente para garantizar el éxito. Incluso si era imprescindible recurrir al terrorismo colectivo, este debía practicarse con el mínimo número de colaboradores (Arias Gil, 2018).

Las células muy pequeñas o de una sola persona que actúen de forma independiente son un verdadero problema para las fuerzas y cuerpos de seguridad y los servicios de inteligencia (Arias Gil, 2018). Cuando se enfrentan a una estructura piramidal clásica, su esfuerzo se centra en "cortar la cabeza", es decir, eliminar la cúspide para así acabar con el grupo. En cambio, el enfrentamiento contra una resistencia sin líderes se hace sumamente complejo pues se compone de un conjunto de cabezas. Cortarlas no implicará la caída del movimiento terrorista, y la escasa o nula relación entre ellas no permitirá saber cuando el enemigo ha sido derrotado por muchas células que se desarticulen. Por otra parte, la resistencia sin líderes es mucho más flexible y permite aumentar el número de atentados, maximizando el daño contra el Estado y la población civil (*Ibid*). Posteriormente, los supremacistas blancos Alex Curtis y Tom Metzger utilizaron por primera vez el concepto de "lobo solitario". La visión de Metzger de esta nueva estrategia es especialmente interesante ya que considera que el lobo solitario debe ser alguien que actúe totalmente en la clandestinidad, alguien que no muestre su ideología públicamente, que oculte su proceso de radicalización y limite sus contactos con otros individuos que compartan su pensamiento. Esto no sólo dificultará la detección del terrorista, sino que incluso podría permitir su acceso a las instituciones gubernamentales, haciendo alusión a los llamados caballos de Troya. El yihadismo también ha recurrido a la estrategia del terrorismo individual. Mustafá Setmarian, también conocido como Abu Musab al-Suri, en su obra *The Global Islamic Resistance Call* hizo referencia al concepto de *Nizam, la Tanzim* -Sistema, no organización- que presenta las mismas ventajas que la resistencia sin líderes de Louis Beam. La complejidad de actuar a través de células en Occidente ha provocado que Al-Qaeda e ISIS argumenten que no es necesario viajar a Oriente Medio para combatir a los infieles. Se puede hacer mucho daño y generar miedo de la forma más simple, con un arma blanca o un vehículo. En su ideario, si no es posible realizar la Hégira hacia el califato, el musulmán tiene la obligación de hacer la yihad allí donde esté. Además, el terrorismo individual es una táctica efectiva según estos grupos ya que crea un estado de terror y ansiedad en la sociedad victimizada (Toboso, 2015) y una situación de confusión para los servicios de inteligencia por el gran número de falsos positivos, teniendo en cuenta que cualquier ciudadano podría ser un terrorista individual.

El aumento de casos de terrorismo individual no solo se debe a las ventajas operativas antes presentadas, sino que también resulta más atractivo a nivel psicológico para el propio autor de la violencia. La creciente conflictividad social, el debilitamiento / fragmentación de los marcos identitarios tradicionales -como el nacionalismo, la ideología política o la religión- y la aparición de las redes sociales -donde la cuenta personal lo es todo- han provocado que, de forma generalizada, se ponga toda la atención en el "yo" y haya un desistimiento en

sumarse a un esfuerzo colectivo (González, 2021). El individualismo hace que cada vez más personas no sean reconocidas por su afiliación a un determinado grupo, sino por su "franquicia humana" (Toboso, 2022). El concepto de franquicia humana -o marca personal- está formado por una singular y única forma de percibirse a uno mismo y de percibir al entorno… Se trata de una ideología individualizada que identifica a la persona y la separa de otros. La incapacidad de destacar sobre el resto en términos de popularidad implica que la franquicia humana no será realmente única o conocida. Por supuesto, esto no tendrá importancia para ciertos individuos, pero otros con un carácter narcisista verán cómo se daña su autoestima y sentirán frustración. Algunas personas de este segundo grupo optarán por hacer uso de la violencia para aliviar dicha frustración, incluida la comisión de un acto terrorista. En este sentido, la violencia individual es una herramienta excelente para este fin. Pertenecer a un grupo terrorista reduce el nivel de protagonismo o relevancia del individuo en el acto, en cambio, la imagen de "sólo ante el peligro" alimenta el ego notablemente, especialmente por la repercusión del individuo en redes sociales y medios de comunicación. Louis Beam ya advirtió de esto: el terrorismo individual genera individuos empoderados capaces de obtener reconocimiento y prestigio social dentro de la subcultura extremista a la que pertenecen (Arias Gil, 2018). En su informe de 2017, el grupo de trabajo *RAN Health and Social Care* declaró que el terrorismo individual es la opción para aquellos que se consideran humillados por un sistema que los ha reducido a la insignificancia. Con el ejercicio de la violencia, tienen por objetivo llamar la atención y forzar a la sociedad a ver el mundo desde su perspectiva, es decir, pretenden difundir su "ideología individualizada". Esto queda ejemplificado por el hecho de que, de 120 casos de terroristas individuales estudiados por el grupo, el 70% intentó emitir -ya sea online u offline- sus acciones para así generar un efecto "bola de nieve" en los espectadores. Por otra parte, el individuo contemporáneo tiende a percibir el mundo en las matizaciones de sí mismo y la consecuencia de ello es que el *«otro»* desaparece y deja de interesarle (Toboso, 2022). Si como se ha dicho antes, ciertas personas se decantan por recurrir a la violencia para trascender, es comprensible que opten por actuar independientemente en lugar de formar parte de una organización, con todos los compromisos sociales que ello conlleva. El terrorista individual es fruto del egoísmo, no ha de impregnarse de valores altruistas, como la lealtad a los líderes y el sacrificio por los compañeros.

Pese a todo lo anterior, la estrategia del terrorismo individual sufre de dos graves vulnerabilidades: la austeridad logística y el amateurismo táctico (Toboso, 2019, 63). Hay excepciones a esta afirmación, como el particular caso de Anders Breivik, que el mismo día hizo estallar una bomba en Oslo e inició un tiroteo en la isla de Utoya, causando en total casi un centenar de víctimas. Breivik planificó el ataque durante años, reuniendo fertilizante

para fabricar el explosivo y consiguiendo un uniforme policial para generar confusión en la isla (*La Policía Eleva a 92 Los Muertos Por El Doble Atentado En Noruega*, 2011). Pero por lo general, los terroristas individuales no cuentan con los mismos recursos ni conocimientos que una organización, por lo que sus atentados tendrán una letalidad menor o incluso existen más probabilidades de fracasar. El terrorista individual, como hemos visto, escoge sus medios, tácticas y objetivos libremente, pero en realidad el hecho de que no pertenezca a una red o a una estructura le limita enormemente en dicha elección. Por una parte, en la mayoría de casos de actores solitarios hay una predilección por las capacidades o medios "blandos", es decir, por el uso de armas blancas o vehículos (Toboso, 2015). Esto se debe a que la obtención de armas de fuego y materiales para fabricar explosivos es una tarea compleja para una sola persona, ya sea por el coste o una mayor dificultad para acceder a las redes ilegales de suministradores. Pero ya el mero intento de aumentar la capacidad logística rompe la norma fundamental del terrorista individual de la que hablaba Metzger: el hermetismo y la clandestinidad. Tanto la interacción con terceros como la compra de productos sospechosos generan rastros que facilitan la detección del individuo por parte de los servicios de inteligencia antes incluso de que lleve a cabo el atentado. Por otra parte, aunque la persona haya logrado esquivar a los servicios de inteligencia y cuente con mayores capacidades logísticas que un simple machete o un vehículo pesado, no implica necesariamente que les vaya a dar un buen uso. En su artículo *"Bombing Alone: Tracing the Motivations and Antecedent Behaviors of Lone-Actor Terrorists"* (2013), Paul Gill, John Horgan y Paige Deckert realizaron un análisis de las características sociodemográficas y antecedentes de 119 terroristas individuales. Únicamente el 26% contaba con experiencia militar, y de este subgrupo tan solo el 23,3% había participado activamente en combate. El 41,2% de la muestra había tenido antecedentes criminales. Algunas de las ofensas consistían en actos que en realidad requerían de conocimientos útiles no solo para un delincuente, sino también para un terrorista individual -uso de armas de fuego, uso criminal de explosivos, asesinato, falsificación-, sin embargo, la mayor parte implicaba actos de vandalismo, hurtos, posesión de drogas, posesión de pornografía infantil, conducción bajo los efectos del alcohol, etc. De toda la muestra, solo el 21% había recibido formación práctica, mientras que el 46,2% se había entrenado a través de medios virtuales.

Lo que demuestran estos datos es que una pequeña cifra de los terroristas individuales cuenta con experiencia real, mientras que el resto se entrena online a través de manuales o vídeos -los cuales no ofrecen el mismo nivel de conocimientos- o directamente no cuenta con ningún tipo de formación. Como resultado, se producen atentados sin éxito o poco sofisticados, con individuos que no manejan con precisión el arma o con explosivos defectuosos que estallan en el peor momento -para el terrorista- o que no llegan a hacerlo

(Béthencourt, 2017). Por esta razón, los actores solitarios prefieren objetivos civiles poco ambiciosos (Gill et al., 2013) y medios sencillos / blandos. La mayoría de atentados de este tipo produce un bajo número de víctimas, y aunque cumplen el objetivo esencial del terrorismo, que es generar un mensaje y difundir el miedo entre la sociedad objetivo, es indudable que existe un deseo de causar un mayor daño material. Sin embargo, las dificultades para viajar a campos de entrenamiento en zonas de Oriente Medio, África o Asia genera una dependencia hacia el medio virtual. Es aquí donde los videojuegos y las tecnologías del entretenimiento pueden resultar útiles para cubrir el déficit de habilidades en los terroristas individuales y diversificar los medios que estos pueden emplear.

BLOQUE II. Nuevas tecnologías del entretenimiento y potencial formativo en el ámbito del terrorismo

5. *Serious games*, simuladores y realidad virtual

Aunque la sociedad actual tiende a trivializar la importancia del juego, desde hace milenios se ha utilizado para educar, desarrollar el pensamiento estratégico y para fomentar el trabajo en equipo o el espíritu competitivo (Miller, 2004, como se citó en Smith, 2013). Por ejemplo, los abstractos juegos de tablero como *Go, Chaturanga* o el ajedrez eran comúnmente empleados para instruir a estrategas militares. Con el nacimiento de los videojuegos a mediados del siglo XX el interés por dotarles de potencial formativo fue aumentando progresivamente. Pero lejos de estancarse en los videojuegos educativos para el público infantil, la industria de los *serious games* ha ganado relevancia en múltiples ámbitos profesionales. De hecho, *serious game* es un concepto generalmente definido como "juego diseñado principalmente para perseguir una finalidad distinta al puro entretenimiento". La ambigüedad de la descripción es intencional y responde a la adaptación de esta tecnología a diferentes campos: el empresarial, educativo, sanitario, científico, político, militar, policial, etc. (Smith, 2013).

En el bloque anterior fueron presentadas las ventajas de los videojuegos como factor de radicalización. Diversos elementos, como la diversión o la percepción de autoeficacia, generan satisfacción en el jugador, lo cual le empuja a sumergirse totalmente en el mundo virtual. En realidad, esto resulta útil en cualquier proceso formativo, pues el aprendizaje es mucho más efectivo cuando detrás hay una motivación intrínseca. Pero el auge de los *serious games* no solo se debe a su naturaleza estimulante. Los *serious games* pueden exponer al usuario a una gran variedad de situaciones, algunas difíciles de reflejar fuera del plano digital. Esto es especialmente cierto en lo que se refiere a la preparación de primeros intervinientes en situaciones de emergencia: la organización de un simulacro de atentado o desastre natural depende de la cantidad de actores y de la disponibilidad de una ubicación idónea. Dicho inconveniente puede ser superado gracias al constante avance tecnológico y a sistemas capaces de crear entornos cada vez más realistas, permitiendo incluso la participación simultánea de múltiples usuarios en el entrenamiento (Akhgar, 2019, 10). Precisamente la posibilidad de recrear escenarios sin coste alguno -más allá de la adquisición del sistema- e independientemente del lugar permite que el usuario entrene de forma reiterada hasta alcanzar la perfección sin temor a cometer errores. Los *serious games* son instructores virtuales con una paciencia infinita, cuyo *feedback* instantáneo incentiva al

usuario a seguir el proceso de formación (Federation of American Scientists, 2006). La experiencia previa en el uso de videojuegos también es un factor que ha influido en la extensión de los *serious games*. El éxito de cualquier método de entrenamiento depende de tres factores: la calidad del programa formativo, el contexto en el que el entrenamiento tiene lugar y la familiaridad del aprendiz con el medio empleado. Del mismo modo que no se puede educar con un libro a un individuo analfabeto antes de que aprenda a leer, los *serious games* no pueden ser utilizados como medio de entrenamiento si el usuario nunca ha tenido contacto con algún tipo de videojuego (Orvis et al., 2010). Pero la popularización de la industria del videojuego y el desarrollo de tecnologías *user friendly* han hecho que esto sea un problema residual, siendo las sesiones de adaptación previa al medio cada vez menos necesarias.

En este apartado se presentará un conjunto de *serious games* -la mayoría utilizados en el campo de la seguridad- con el objetivo de examinar sus prestaciones y posible evolución, lo cual es crucial antes de determinar sus posibles usos en el terrorismo. Es necesario aclarar que el concepto de *serious game* es muy amplio e incluye a todo aquel videojuego con fines formativos, independientemente de su grado de sofisticación y sus requisitos técnicos. Sin embargo, para facilitar el estudio de los ejemplos seleccionados estos han sido clasificados entre *serious games* "básicos", simuladores avanzados y *serious games* basados en la tecnología VR. Las dos primeras categorías recurren al teclado, mientras que la tercera hace uso de *hardware* de realidad virtual. Para distinguir a *serious games* "básicos" de simuladores avanzados se ha utilizado una clasificación inspirada en la comparación de Thiagarajan (1998) entre *high-fidelity simulations* y *low-fidelity simulations*. Los simuladores avanzados son el equivalente a las *high-fidelity simulations*, las cuales incorporan una gran cantidad de elementos para recrear de la forma más realista posible el proceso instructivo. Permiten un alto grado de interacción con el entorno o los artefactos representados virtualmente. Un claro ejemplo son los simuladores de vuelo, donde el usuario lleva a cabo su entrenamiento dentro de una cabina de piloto. Por el contrario, los *serious games* "básicos" son el equivalente a las *low-fidelity simulations*, las cuales ofrecen una representación simplificada de la realidad y ponen el foco de atención en ciertos elementos principales del proceso. La interacción con el entorno es reducida intencionalmente para que el jugador se centre en la adquisición de conocimiento teórico. Aquí se incluyen *serious games* donde el usuario se limita a escoger entre múltiples opciones como si de un test se tratara. Otra perspectiva de distinción entre *serious games* "básicos" y simuladores avanzados es el grado de ludificación. Los primeros tienden a incorporar elementos que promueven la motivación intrínseca, como un sistema de logros, *rankings*, efectos visuales agradables, etc. En cambio, los simuladores avanzados generalmente prescinden de estos

complementos ya que, por una parte, pretenden ser fieles a la realidad, y por la otra, se entiende que serán utilizados por usuarios altamente motivados previamente (Atkinson-Bonasio, 2008).

5.1. Serious games "básicos"

Es fácil encontrar simuladores de baja fidelidad adaptados a cualquier tipo de ámbito. Sus mecánicas de juego simples, frecuentemente basadas en el *point and click* con el ratón, son ideales para usuarios con poca experiencia o para instruir en conceptos teóricos. Su popularidad ha aumentado especialmente en el campo de la ciberseguridad, donde se han desarrollado multitud de *serious games* orientados a la ciudadanía y las PYMES para fomentar medidas de autoprotección digital básicas. Un ejemplo de ello es *CyberCentric*, un sencillo simulador que presenta su contenido educativo en forma de narrativas y escenarios relacionados con ciberataques en el seno de una PYME. El jugador debe contestar a una serie de preguntas teniendo en cuenta aspectos como los recursos, la reputación y la resiliencia de su empresa (*CENTRIC Cyber Winning National Awards*, 2019). Los *serious games* no solo resultan de utilidad para concienciar a usuarios con pocos conocimientos a la hora de evitar riesgos digitales, sino que también han sido empleados por profesionales en la materia. En el ámbito de la ciberseguridad se distingue entre *blue teams,* cuya misión es la de mejorar la protección de redes y sistemas informáticos ante diferentes amenazas, y *red teams*, encargados de llevar a cabo ciberataques con el objetivo de detectar vulnerabilidades y recomendar soluciones -lo que se conoce como hacking ético o *penetration testing*-. Ambos tipos de expertos necesitan actualizar constantemente sus conocimientos, por ello realizan ejercicios en escenarios virtuales simulados o *cyber-ranges*. Se trata de redes ficticias donde *blue teams* y *red teams* pueden mejorar sus habilidades técnicas de forma práctica. Sin embargo, estos escenarios tienden a ser construidos "manualmente", lo que resulta lento y costoso. Por esta razón, se han desarrollado *serious games* que tratan de reflejar los ejercicios llevados a cabo en *cyber-ranges*, pero de forma simplificada en escenarios prediseñados, como *X-Hacker* o *Red vs Blue: Cyber-Security Simulator*. El primero instruye al jugador en los principios del hacking ético a través de una serie de niveles que representan diversas topologías de red (Alhadeff, 2019), el segundo consiste en una competición en línea donde *red team* y *blue team* operan simultáneamente en niveles donde el tiempo y los recursos son limitados (Yamin et al., 2021).

En materia de seguridad policial los *serious games* también han sido utilizados con distintas finalidades. *Unravel the Mysterious Murder* prepara a los agentes para llevar a cabo investigaciones forenses en un escenario virtual donde se ha cometido un asesinato. El

jugador deberá inspeccionar el lugar, recolectar pruebas y realizar análisis de huellas dactilares o muestras de sangre para determinar que sospechoso es culpable del crimen. El sistema está programado para que cada vez que sea iniciado sus elementos principales -víctima, culpable, lugar de los hechos o pruebas en el escenario- cambien aleatoriamente, ofreciendo al jugador una experiencia de dificultad variable (Drakou & Lanitis, 2016). ISPO (*Interview Skills for Police Officers*) tiene por objetivo mejorar las habilidades de comunicación relacionadas con interrogatorios a sospechosos, testigos o víctimas. El juego se compone de una serie de interrogatorios simulados donde el jugador debe seleccionar las opciones -predeterminadas- de diálogo correctas para obtener el máximo de información posible al mismo tiempo que controla el estado emocional del interrogado. Además, en ciertas ocasiones el interrogado tratará de manipular al jugador aportando datos falsos. Para determinar la veracidad de la información se debe observar el lenguaje no verbal del interrogado, ya sea a través de expresiones faciales o lenguaje corporal (Guimarães et al., 2022). La planificación de intervenciones en las que el uso de la fuerza es requerido es abarcada en *Door Kickers: Simulations & Training*, donde los usuarios han de lograr que un equipo SWAT penetre en un edificio ocupado por criminales o terroristas y cumpla una determinada misión, ya sea el rescate de rehenes o la desactivación de una bomba. El jugador debe posicionar a sus unidades en los puntos que considere más adecuados para asaltar el edificio, que es mostrado en forma de plano arquitectónico. Tras esto, con el ratón puede guiar el movimiento y la zona de apuntado de los agentes virtuales, que abrirán fuego automáticamente en cuanto detecten a un enemigo. Aunque la misión transcurre a tiempo real, se da la posibilidad de pausar y observar el escenario para poder reaccionar a nuevas amenazas (Simpson, 2014). Por otra parte, la ludificación también ha sido empleada en métodos educativos sobre principios de la policía comunitaria, como *AEsOP*. A través de doce escenarios, cada uno relacionado con distintos tipos de criminalidad, el jugador debe ponerse en el papel de diversos actores comunitarios -incluyendo la policía- y tomar distintas decisiones para prevenir o reducir el impacto de los problemas que afectan a los ciudadanos. En este sentido, el juego funciona como una novela visual interactiva, con múltiples opciones disponibles y, por lo tanto, varios desenlaces.[11]

En un contexto militar, *Elect BILAT* fue utilizado por el ejército estadounidense para desarrollar habilidades de negociación en contextos culturales específicos, especialmente de Oriente Medio. El usuario deberá recolectar información sobre los intereses y necesidades de su interlocutor mientras escoge las opciones de diálogo correctas para no generar rechazo. Lo interesante de este simulador es que, por una parte, las negociaciones

[11] AEsOP – CENTRIC

no son ejercicios aislados, sino que forman parte de una narrativa continua donde la construcción de confianza, el tiempo y los recursos son factores a tener en cuenta. Por otra parte, insiste en la comprensión de las convenciones culturales y las costumbres de la zona -por ejemplo, el acto de quitarse el casco y las gafas de sol antes de iniciar una conversación- para lograr mejores resultados en la negociación (Hill et al., 2006). En realidad, los *serious games* básicos han sido utilizados desde hace décadas por distintos ejércitos, sobre todo como simuladores de decisiones tácticas en situaciones críticas. En este sentido destaca *Close Combat Marine*, *serious game* perteneciente a la saga comercial del mismo nombre pero adaptado a las necesidades específicas del cuerpo de marines estadounidense. CCM es un simulador de combate táctico a tiempo real donde el jugador debe guiar a múltiples unidades de infantería en una serie de enfrentamientos. Para ello posee una visión general del escenario y un cuadro de órdenes que puede emitir fácilmente con el ratón, desde el desplazamiento hasta atacar a un enemigo. El éxito depende de la aplicación de tácticas militares realistas, por ejemplo, situar a las unidades en coberturas adecuadas, ejercer fuego de supresión o realizar maniobras de flanco (Nichols, 2019).

Por último, en la vertiente del contraterrorismo se han implementado videojuegos destinados a miembros de los servicios de inteligencia para mejorar su capacidad de detección y predicción. *PROACTIVE* es un juego de estrategia por turnos esencialmente basado en la lógica de *red team* y *blue team*, pero adaptado a un enfrentamiento entre cuerpos de seguridad y terroristas. En función del bando seleccionado el jugador deberá ejecutar con éxito el ataque a una localización o, por el contrario, prevenirlo. El bando terrorista ha de completar una serie de fases preparatorias antes de llevar a cabo el asalto -observación de la localización en vehículo o a pie y evaluación de la seguridad-. Por su parte, el jugador que controle a los cuerpos de seguridad debe identificar información relevante generada durante las fases preparatorias llevadas a cabo por los terroristas para determinar cuándo y dónde atacarán (Sormani et al., 2016). *Sibilla* introduce un enfoque diferente, pues los jugadores actuarán como operadores de distintos servicios de inteligencia antiterrorista. El juego se centra en representar la importancia de llevar a cabo un análisis correcto de la información recolectada para así poder tomar decisiones eficaces. Al mismo tiempo, se debe afrontar la presión del tiempo y las insuficiencias de presupuesto. También es útil para fomentar la colaboración y negociación entre las organizaciones controladas por múltiples jugadores (Bruzzone et al., 2009).

5.2. Simuladores avanzados

Los simuladores de alta fidelidad llevan utilizándose desde mucho antes que los *serious games* básicos o los sistemas de realidad virtual, véase la primera versión de *Microsoft Flight Simulator*, lanzada en 1982. Mientras que los *serious games* básicos dan mayor importancia a los controles sencillos y al conocimiento cognitivo / teórico, los simuladores avanzados son sumamente detallados e incluso complejos -hasta el punto de que algunos serían inoperables por individuos inexpertos- ya que pretenden instruir a los usuarios en procedimientos, técnicas o el empleo de mecanismos e instrumentos realistas. Es decir, los simuladores avanzados pretenden mejorar las capacidades prácticas. Han logrado integrarse fácilmente en campos profesionales donde la ejecución de ejercicios fuera del plano virtual resulta costosa o peligrosa. Pero en los últimos años ha habido un crecimiento en la popularidad de estos programas, por lo que han proliferado simuladores comerciales destinados a un público que simplemente desea experimentar un *gameplay* más realista que el ofrecido por los videojuegos ordinarios. Por ejemplo, *DIY Simulator* está orientado a la fabricación de objetos caseros y de bricolaje, como patinetes eléctricos, drones, altavoces, etc. Aunque el sistema de ensamblaje es *user-friendly* ya que el jugador simplemente ha de arrastrar los materiales necesarios a los espacios resaltados con colores, resulta interesante ya que explica paso a paso cómo alcanzar el resultado final y las herramientas necesarias para ello.[12] En el mismo sentido, *The Workshop Game* sitúa al jugador en un taller virtual donde debe utilizar maquinaria y herramientas diversas para producir un componente particular en base a unos diseños predeterminados. A diferencia de *DIY Simulator*, *The Workshop Game* trata de virtualizar procesos y maquinaria reales, además de tener en cuenta sugerencias de expertos en la materia (Horejší et al., 2019). De forma similar, *Car Mechanic Simulator*, tal y como su nombre indica, ofrece al usuario la posibilidad de gestionar su propio taller de automóviles, pudiendo repararlos o modificarlos. La última edición es una de las mejores en el mercado, pues muestra con gran exactitud los componentes internos y externos de hasta 72 vehículos distintos. El jugador debe interactuar con estos componentes para satisfacer los criterios de los encargos realizados por sus clientes (*Car Mechanic Simulator: How Realism Is Best for Education*, 2021). *Gunsmith Simulator* mantiene la esencia de *Car Mechanic Simulator* pero aplicada a armas de fuego: el jugador simulará ser un armero que, en función de los encargos recibidos, deberá desmontar, limpiar, reparar o añadir complementos a una amplia variedad de armas también representadas con todo lujo de detalles.[13] Por último, en la industria de los simuladores comerciales han ganado peso los simuladores de vuelo de drones. Estos

[12] DIY Simulator on Steam
[13] Gunsmith Simulator - Game Hunters

permiten controlar diferentes tipos de drones -e incluso importar modelos digitales personalizados- en múltiples escenarios capaces de reflejar condiciones físicas y meteorológicas realistas. La experiencia puede ser mejorada si el usuario decide conectar un control remoto al dispositivo informático para así utilizarlo en la simulación (*Drone Flight Simulators: Your Guide to the Top 8 Drone Simulators of 2022*, s.f.).

Los ejemplos anteriores no son empleados con fines de mejora profesional, pero han sido mencionados ya que poseen una calidad notable o tratan conceptos poco explorados en el sector del entretenimiento. Pese a ello, son los simuladores militares los que reciben mayor atención y recursos en su desarrollo. Algunos permiten al usuario formar parte de la tripulación de un vehículo blindado o aéreo. Este tipo de simulaciones trata de reflejar fielmente su interior y todos sus sistemas para que el jugador se acostumbre antes de ponerse al mando de un vehículo real. En cambio, otros se enfocan en el entrenamiento de infantería, por lo que el jugador controla al avatar de un individuo en particular, como si se tratara de un *first person shooter* pero mucho más sofisticado. Uno de los primeros y más exitosos fue *DARWARS Ambush!*, una simulación en primera persona donde múltiples usuarios -conectados *online*- debían escoltar un convoy militar por zonas inspiradas en Irak y Afganistán. El bando enemigo, cuyo objetivo era la destrucción del convoy, estaba formado por insurgentes, que podían ser controlados por la IA u otros jugadores (Robson, 2006). Pero *DARWARS Ambush!* ha terminado siendo superado por *Virtual Battlespace* (VBS). VBS mantiene la base de *DARWARS* pero con un enfoque más amplio, no solo en su variedad de misiones, sino también porque permite la colaboración entre infantería y vehículos, también controlados por los jugadores. Los puntos fuertes de VBS son tres: nivel de interacción con el espacio virtual, variedad de escenarios y calidad de la inteligencia artificial. Por una parte, en VBS el usuario -que actúe como una unidad de infantería- no solo abrirá fuego[14] o desplazará a su avatar, sino que también puede interactuar con el entorno y ejecutar un conjunto de acciones que reproducen cualquier movimiento que el combatiente pudiera realizar en la vida real, como esconderse detrás de coberturas, desactivar explosivos improvisados, desplegar equipo defensivo -alambradas o sacos de arena-, dar órdenes a los subordinados o arrastrar a compañeros heridos hasta un lugar seguro. Por otra parte, los escenarios tridimensionales pueden incluir desde desiertos o zonas deshabitadas hasta núcleos urbanos llenos de población civil. El simulador incluye una herramienta de edición de mapas para que los instructores los modifiquen y adapten a

[14] El apuntado se hace mediante el ratón, por lo que este tipo de simuladores no instruyen en el manejo del arma, sino que fomentan la coordinación ojo-mano (Samčović, 2018), la adquisición rápida de objetivos y generan estímulos asociados a la necesidad de abrir fuego para posteriormente facilitar la respuesta violenta (Grossman, 1998).

las necesidades específicas de los usuarios.[15] De hecho, la versión más reciente de VBS incluye un *software* que, en base a imágenes y datos satelitales, puede generar réplicas realistas de prácticamente cualquier parte del mundo.[16] Los entornos jugables pueden verse alterados durante el transcurso de la simulación, ya sea por las explosiones o impactos de bala capaces de deformar y destruir infraestructuras o por las condiciones meteorológicas variables. Por último, VBS introduce una inteligencia artificial avanzada e integrada tanto en los combatientes como en la población civil. La calidad de la IA facilita la inclusión de más personajes "secundarios" en el escenario y hace que reaccionen de forma realista a los estímulos. Los instructores pueden determinar las conductas de estos personajes no controlados por humanos antes y durante la misión (Sánchez Morales, 2020, 16). Eventualmente, el éxito comercial de los MMO (*massively multiplayer online games*) hizo que creciera el interés por transformar a los simuladores militares en mundos virtuales activos 24/7. Un proyecto orientado a este fin fue *Asymmetric Warfare: Virtual Training Technology*. Al igual que cualquier MMO, este nuevo simulador contaba con un sistema de servidores online que permitía la existencia -permanente- de un único escenario masivo. Los jugadores podían conectarse en cualquier momento y desde cualquier dispositivo para adoptar un determinado rol -militar estadounidense, insurgente o civil-. En realidad, *Asymmetric Warfare* no difiere en gran medida de *DARWARS* o VBS, pero introduce un concepto nuevo que es el de la continuidad: los ejercicios llevados a cabo no son actos aislados, sino que tendrán consecuencias en posteriores sesiones por lo que la planificación a largo plazo es importante (Peck, 2005).

Para finalizar este subapartado, es necesario recalcar que no todos los simuladores de alta fidelidad empleados en el ámbito militar se centran en el combate. Por ejemplo, en *3D SanTrain* los usuarios deben practicar primeros auxilios sobre un herido en combate. Para ello cuentan con diferentes instrumentos médicos y una representación realista de la fisiología humana (Dobrovsky et al., 2017).

5.3. Realidad virtual

Los sistemas de realidad virtual pueden consistir en simuladores de baja o alta fidelidad. Su principal característica es que no son operados mediante teclado y ratón, sino a través de *hardware* adicional que registra y reproduce los movimientos corporales en el plano físico,

[15] La estrategia seguida en *Six Days in Fallujah* -*shooter* táctico destinado al público general- también resulta interesante. En lugar de diseñar escenarios, sus creadores han elaborado un sistema de arquitectura procedural, por lo que en cada partida el mapa se ve modificado. De esta forma se evita que los jugadores memoricen el entorno (Coombes, 2021).
[16] VBS4 | BISim

transformándose así en el método de interacción con la simulación. En otras palabras, mientras que en los *serious games* mencionados anteriormente los usuarios observaban el escenario virtual desde detrás de una pantalla, la realidad virtual directamente los "sumerge" en un escenario donde el límite de acciones disponibles es marcado por su propio cuerpo. En este sentido, se ha de diferenciar entre sistemas de realidad virtual no inmersiva y sistemas de realidad virtual inmersiva, pues ofrecen un grado distinto de interacción (de Armas et al., 2020).

La realidad virtual no inmersiva es aquella donde el escenario[17] es proyectado a través de pantallas situadas en paredes, techo y suelo. Tales pantallas pueden rodear totalmente al usuario o situarse en frente suyo. Un conjunto de sensores captará sus movimientos, los cuales quedarán representados en la pantalla y serán los que hagan avanzar la simulación. Los sistemas de RV no inmersivos se han popularizado especialmente por su uso como "galerías de tiro", por ejemplo, el simulador de tiro *VIRTRA* empleado por el cuerpo de Mossos d'Esquadra (Díez Cámara, 2021). El usuario empuña réplicas de armas de fuego que, al ser disparadas, emiten una señal a los sensores. En función del ángulo de tiro y la posición del usuario, los sensores determinarán si el proyectil "virtual" ha impactado en los blancos fijos / móviles o individuos hostiles mostrados por la pantalla. Algunas de estas réplicas incluso poseen mecanismos para simular el retroceso del arma. Otros sistemas de RV no inmersivos son más versátiles y registran un mayor número de acciones. En *Sidh* -simulador destinado al entrenamiento de bomberos- el objetivo es adentrarse en una infraestructura en llamas y rescatar a los afectados. Los sensores reconocen cuando el usuario corre, se agacha, mueve los brazos o recoge a un herido (Backlund et al., 2007).

Los sistemas no inmersivos facilitan el entrenamiento al usuario sin experiencia previa en realidad virtual y evitan el efecto negativo de la *cybersickness*. Sin embargo, lentamente ganan peso los sistemas de realidad virtual inmersivos, principalmente por el hecho de que permiten construir escenarios altamente interactivos y no se limitan a mostrar dianas virtuales en espacios inanimados o escenas pregrabadas. En los sistemas inmersivos, el usuario se integra totalmente en el entorno 3D gracias a visores estereoscópicos, también conocidos como gafas de realidad virtual. Estos dispositivos aíslan al individuo que los porta, pues las imágenes y el audio emitido captan toda su atención. Los sistemas de RV inmersivos más básicos requieren de controladores manuales para ser operados. Estos incluyen botones, gatillos y *joysticks* utilizados para reflejar el movimiento de las manos,

[17] Algunos de estos sistemas no transcurren en entornos 3D, sino que muestran escenas pregrabadas que toman diferentes rumbos en función de las acciones del usuario, como si se tratara de un vídeo interactivo.

interactuar con objetos o desplazarse por el entorno. Pero la tecnología avanza a un ritmo avanzado y hoy en día ya existen proyectos para mejorar la experiencia gracias a cintas de correr omnidireccionales, guantes de RV y trajes hápticos. Por una parte, las cintas de correr omnidireccionales, tal y como su nombre indica, permiten al usuario caminar, correr, saltar y agacharse en cualquier dirección. Este movimiento en el plano físico se traducirá al entorno virtual. De esta forma se abandonaría el desplazamiento clásico basado en palancas de control (Rus, 2020). Por otra parte, como se ha indicado anteriormente se suelen utilizar controladores manuales con botones para simular el movimiento de las manos y los dedos. El problema es que esto da lugar a interacciones poco naturales, complejas y sin ningún tipo de *feedback* físico. Por esta razón ya se han ideado guantes con sensores integrados para que los movimientos que hace el usuario con sus manos sean directamente reflejados en la simulación. Además, estos guantes contienen actuadores microfluídicos que desplazan físicamente con aire comprimido la piel del usuario cuando interactúa con objetos virtuales (*HaptX Abre La Pre-Compra De Sus Guantes Gloves G1*, 2022). Por último, los trajes hápticos son el último paso para que los escenarios virtuales dejen de ser imágenes intangibles. Investigadores del Instituto Hasso-Platner en Alemania crearon en 2018 un prototipo de traje háptico que estimula los músculos a través de corrientes de baja intensidad. Tal estimulación permite sentir el peso de un objeto virtual o el esfuerzo que se debe hacer al desplazarlo. Esto supone una oportunidad excelente para desarrollar simuladores de tiro más realistas donde el usuario pueda sentir el retroceso del arma[18] o su postura sea corregida gracias a estímulos automáticos (Hayden, 2018). Pero sus capacidades pueden ir mucho más allá. Para el proyecto AUGGMED -será explicado a continuación- se desarrolló un traje háptico que ofrece tres tipos de *feedback*. Los motores de vibración manifiestan el contacto físico con un objeto sólido del entorno virtual, sea una pared o una persona. Los actuadores térmicos aumentan la temperatura del traje cuando el usuario se aproxima a una fuente de calor. El traje contaba además con una serie de actuadores que indican al usuario cuando ha sido impactado por un proyectil en un escenario donde se haya hecho uso de armas de fuego (Akhgar, 2019, 114). Mientras que los avances tecnológicos en *serious games* básicos y simuladores avanzados se centran, principalmente, en perfeccionar sus gráficos o potencia -con tal de incluir escenarios de mayor tamaño-, el futuro se muestra muy favorable al ámbito de la realidad virtual, que disfrutará de innovaciones verdaderamente significativas en su funcionamiento.

[18] De hecho, en Wei et al. (2019) se presenta un traje háptico capaz de generar el retroceso y el peso del disparador -que determinará la fuerza necesaria que hay que ejercer con el dedo para manipular el gatillo- adecuados en función del tipo de arma utilizada, lo que incluye su calibre, peso, longitud del cañón, cadencia de fuego, etc.

La tecnología de realidad virtual inmersiva en materia de seguridad ha sido empleada, especialmente, para transmitir al usuario emociones intensas que tendrá que experimentar en el futuro o para facilitar su adaptación a situaciones novedosas. Por ejemplo, *BraveMinds* recrea un escenario con un alto grado de realismo en el que los usuarios -veteranos de guerra que sufren de trastorno por estrés post traumático- pueden afrontar las memorias traumáticas con ayuda de terapia profesional. El sistema no solo emplea gafas de realidad virtual, sino que también incluye mecanismos para replicar olores, como el de objetos quemados o sudor (Haskins, 2020). En 2017, el Estado de Colorado introdujo un programa de reinserción destinado a convictos encarcelados durante más de 20 años. Dado que muchos de estos individuos ingresaron en prisión en un contexto totalmente distinto al actual, se decidió ofrecer sesiones de realidad virtual para mostrarles los avances sociales y tecnológicos que encontrarán tras su liberación. En la simulación, se solicita a los usuarios que realicen tareas básicas, como comprar en un supermercado o hacer la colada (Dolven & Fidel, 2017). Recientemente, la empresa *AXON* ha creado un simulador donde los usuarios, como agentes de policía, deben actuar correctamente frente a una persona que sufre de una crisis mental. Para ello han de poner en práctica técnicas de desescalada de conflictos (*New Federal De-Escalation Grant Program Will Improve Opportunities for Mental Health Intervention for State & Local Agencies*, 2023). En el futuro, el avance tecnológico permitirá incluir nuevas funcionalidades que mejoren aún más la interacción, como sistemas de verbalización (de Armas et al., 2020). Estos ejemplos demuestran que la realidad virtual es útil para la preparación mental, pero se trata de una tecnología que posee mucho más potencial, por lo que ya está siendo integrada en simuladores de alta fidelidad, cómo AUGGMED. AUGGMED es un proyecto financiado por la UE que consiste en un simulador avanzado donde los usuarios actuarán como primeros intervinientes durante un atentado terrorista, por lo que cabe la posibilidad de que se vean obligados a usar el arma reglamentaria. Para aumentar el estrés típico de estos escenarios, el simulador se complementa con el motor *EXODUS* -para replicar el comportamiento de grandes grupos de civiles huyendo del peligro- y *SMARTFIRE* -el cual genera una evolución realista del fuego, las explosiones y las heridas-.[19]

Para finalizar, otra categoría -mucho menos desarrollada- de realidad virtual es la realidad aumentada. La realidad aumentada consiste en tecnologías -normalmente gafas inteligentes, como *Google Glass*- que proyectan imágenes virtuales superpuestas en la visión que tiene el usuario del mundo real. Estos dispositivos apenas se han adentrado en el mundo de los *serious games* ya que por el momento se centran exclusivamente en lo

[19] Automated Serious Game Scenario Generator for Mixed Reality Training

visual. Son utilizados con mayor frecuencia para mostrar objetos 3D delante del usuario. Por ejemplo, en el campo de la ingeniería esto resulta útil ya que el portador de las gafas puede inspeccionar desde todos los ángulos motores o máquinas y así estudiar su estructura. Pero esto no permite ningún tipo de interacción más allá de la posible selección de ciertos elementos en el objeto para obtener una descripción. Pese a ello, la realidad aumentada presenta características muy interesantes en lo que se refiere a las prácticas de tiro. *URBAN* es el *software* creado y empleado por las fuerzas armadas españolas que combina gafas de RA con fusiles *airsoft.* Las gafas inyectan imágenes virtuales de aliados, enemigos o civiles sobre dianas inteligentes o el entorno físico que rodea al usuario. Un conjunto de sensores determinará si al abrir fuego el blanco ha sido impactado o no (*El Ejército Diseña Un Sistema De Adiestramiento De Realidad Aumentada*, 2019). Incluso se podrían llevar a cabo ejercicios colaborativos con otros participantes aún estando en diferentes localizaciones gracias a la técnica conocida como *holoportation*.[20] En lugar de proyectar imágenes virtuales estáticas, las gafas podrían proyectar modelos 3D de otros usuarios, cuyos movimientos y sonidos serían reproducidos a tiempo real tal y como si se encontraran en el mismo espacio físico.

6. Necesidades formativas del terrorismo

Para determinar cómo los videojuegos podrían ser utilizados por el terrorismo como metodo de entrenamiento, previamente se debe comprender qué necesidades formativas pretenden satisfacer. En este apartado se analizarán las habilidades y conocimientos “deseables” en un terrorista -sin poner el foco de atención en una tipología en concreto-. Las necesidades formativas aquí presentadas son extraídas a partir de la lectura de diferentes manuales de entrenamiento y formación, documentos -impresos o en formato digital- orientados a mejorar la capacidad del individuo para desempeñar una función, incluido el ejercicio de la violencia. De igual forma que los ejércitos de distintos Estados han recurrido a manuales de campo para instruir a sus tropas, el terrorismo también ha empleado esta metodología durante décadas. Su sencillez, bajo coste y amplia difusión -especialmente a partir de la era de Internet- han hecho que ya no sea estrictamente necesario desplazarse a un campo de entrenamiento físico -con todos los riesgos que ello conlleva- para formar parte de un grupo o movimiento terrorista.[21] Consecuentemente, desde hace años abundan en la red

[20] Holoportation™ - Microsoft Research

[21] El mismo Mustafá Setmarian consideraba que, en lugar de ordenar el desplazamiento a campos de entrenamiento en países como Afganistán, era necesario extender la formación a más lugares para que pudiera ser disfrutada por un número mayor de terroristas. Para ello, hizo mención explícita

documentos, enciclopedias, revistas e incluso vídeos de este estilo distribuidos por grupos terroristas, sus filiales regionales o los individuos simpatizantes. Las fuentes procedentes de los grandes grupos o sus filiales -por ejemplo, las revistas *Inspire, Dabiq*, *Majallat al-Fath o Mu'askar al-Battar*- son más populares y generalmente gozan de mayor credibilidad entre sus miembros, incluso presentando información desactualizada en algunos casos. Sin embargo, en la actualidad predominan cuantitativamente los recursos aportados por individuos auto radicalizados a través de foros y chats, tanto de carácter yihadista como de extrema derecha.[22] Pese a ello, su calidad es variable. Encontramos a individuos, como Anders Breivik, en cuyo manifiesto más allá de narrar sus motivaciones también detalla cómo planificar un atentado. Desde aspectos operacionales como las tácticas, los métodos para pasar desapercibido y el armamento a utilizar hasta cuestiones relacionadas con la difusión del mensaje, como la preparación de una sesión de fotos a modo de propaganda (Breivik, 2011). Pero la mayoría se limita a reenviar documentos elaborados por otros actores o incluso se atreven a desarrollar los suyos propios sin contar con los recursos o la experiencia suficientes. Esto último genera un evidente problema ya que los consejos que ofrecerán serán demasiado simples o totalmente incorrectos. En el intento de contribuir a la lucha por su narrativa extremista violenta estos individuos generan un *overflow* de información que dificulta a los principiantes identificar el material instructivo de calidad (Stenersen, 2008).

Aún así, aquí no se entrará en detalles sobre el contenido o instrucciones que ofrecen los documentos para ejecutar una determinada tarea, y tampoco se realizará un estudio comparativo entre ellos. Para la investigación es irrelevante si un manual presenta métodos desactualizados, extremadamente simples o erróneos. La atención se centra en el "qué", en las necesidades formativas que resultan de interés para el terrorismo -según los manuales- y no en el "cómo" pretenden desarrollarlas, pues es evidente que hay variedad de métodos y que los documentos más completos, complejos y de mayor calidad no están disponibles a través de fuentes abiertas. Los manuales que a continuación se presentarán han sido seleccionados ya que abarcan tipologías de atentados que pueden ser preparados por terroristas individuales o células pequeñas y porque desarrollan otro tipo de habilidades que pueden serles de gran utilidad para sobrevivir dentro de la sociedad atacada:

---

al aprendizaje de capacidades militares básicas a través de manuales disponibles en Internet (Abu Mus'ab al-Suri, 2005, como se citó en Stenersen, 2008).

[22] Véase el blog supremacista blanco *Stormfront*, que entre otras cuestiones, dedica un apartado completo al armamento, preparación militar, artes marciales, etc. Self Defense, Martial Arts & Preparedness - Stormfront

- Minimanual del guerrillero urbano (1969). Escrito por Carlos Marighella para guiar las acciones del grupo guerrillero ALN (*Ação Libertadora Nacional*) contra el régimen dictatorial brasileño. Los manuales de grupos guerrilleros y paramilitares han demostrado ser una fuente de inspiración para posteriores campañas insurgentes y terroristas. En el artículo "*The Jihadi Experiences: The Military Theory of Open Fronts*" de la revista *Inspire* (2010) se declaró que para llevar a cabo la yihad era importante estudiar los principios de la guerra de guerrillas desarrollados por teóricos como Mao Tse-Tung, Guevara, Võ Nguyên Giáp y Castro, entre otros (Aarsen, 2017). Se ha escogido el manual de Marighella ya que se diferencia de otros similares, como "La guerra de guerrillas" del Che Guevara, al dejar de lado la guerrilla rural y adaptarla al entorno urbano, centrándose en cuestiones tácticas e individuales, no estratégicas. Por otra parte, mientras que el Che Guevara descartó el terrorismo por ser una táctica que ponía en riesgo el apoyo popular (*Ibid*), Marighella afirmó que no es diferente de otros actos guerrilleros y que no se debe renunciar a esta.

- Sección *Open Source Jihad* de la revista *Inspire*, publicada por Al Qaeda hasta 2017. Aunque la revista es un claro ejemplo de propaganda yihadista, esta sección se dedica a instruir a individuos que simpaticen con la narrativa extremista del grupo y deseen ejercer la violencia en Occidente. Se ha realizado la lectura del artículo "*Lone Wolf Terrorism and Open Source Jihad*" de Claire Wiskind (2016), donde se examinan diez tipos de atentados contemplados en varias de sus publicaciones.

- Primer y segundo volumen del *Green Book,* elaborados por el IRA (*Irish Republican Army*) para preparar psicológicamente a sus miembros ante los interrogatorios y la tortura.

- *Al Qaeda Training Manual* o "manual de Manchester". Este documento fue encontrado en el ordenador de un afiliado a Al Qaeda tras el registro de su domicilio en Manchester, en el año 2000. La escasez de contenido propagandístico en el manual y el hecho de que previamente no hubiera sido publicado o compartido en Internet demuestra que se trata de un documento interno no destinado a atraer nuevos miembros. Además, una de sus primeras páginas declara lo siguiente: "It is forbidden to remove this from the house", siendo la casa una referencia a Al Qaeda (Aarsen, 2017). Está compuesto por 18 capítulos que abarcan técnicas de combate, secuestros, asesinatos con veneno, métodos de tortura, etc. Sin embargo, se ha realizado la lectura de una versión censurada, mostrando únicamente los capítulos

centrados en estrategias para planificar operaciones en Occidente evitando la detección por parte de las agencias de inteligencia.

- *How to survive in the west: A Mujahid Guide*. Este manual fue publicado por una cuenta de Twitter asociada a Estado Islámico en 2015 y desde ese entonces ha sido redistribuido continuamente (*E-Book Distributed Via Twitter: 'How To Survive In The West – A Mujahid Guide'*, 2015). Tal y como su anónimo autor explica, se trata de una guía para los musulmanes que viven en un país o zona de mayoría no musulmana y que necesitan convertirse en "agentes secretos" con una doble vida. En este sentido, comparte muchos puntos en común con el manual de Manchester, pero teniendo una mayor consideración del potencial de Internet y el anonimato digital. Sin embargo, es un documento de una calidad menor y con errores (Gault, 2015). Por ejemplo, aconseja utilizar el sitio web wikiHow para aprender a crear armas rudimentarias, e incluso recomienda ver películas como la saga Bourne para adquirir ideas de espionaje y contraespionaje.

- *Al Qaeda kidnapping manual.* Elaborado por Abdel Aziz al-Muqrin, ex-líder de Al Qaeda en Arabia Saudí (*Al Qaeda Militants Kill American Hostage*, 2004), este manual ofrece información para ejecutar eficazmente y de forma segura secuestros públicos o secretos, así como para mantener a los rehenes.

- 2083: Una Declaración Europea de Independencia (2011). En este compendio de tres libros Anders Breivik expuso sus motivaciones ideológicas para llevar a cabo el doble atentado en Oslo y Utoya, pero también elabora detalladamente su *modus operandi* y ofrece información a nuevos "caballeros templarios" para que sigan sus pasos.

En los próximos subapartados se estudiarán las necesidades formativas incluidas en los manuales anteriores. Muchas de ellas aparecen en múltiples documentos, demostrando que no son exclusivas de un período concreto o una tipología particular de terrorismo, en cambio, tienen un carácter general que resulta de interés para todo aquel individuo o pequeño grupo de personas que aspira a atentar desde dentro de la sociedad objetivo.

6.1. Fabricación de explosivos

Es evidente que la fabricación de explosivos ocupa un lugar prioritario para el terrorismo, independientemente de su motivación. El artefacto en cuestión genera la capacidad de

producir múltiples víctimas y heridos en segundos, dañar las infraestructuras cercanas y generar un estado de confusión y terror que no podrá ser ignorado, especialmente si se producen explosiones simultáneas en distintas localizaciones. Además, permite al autor de los hechos huir antes de que se ejecute el atentado, en caso de que no se trate de un ataque suicida. El potencial destructivo de una bomba hace que muchos individuos se arriesguen a crear una. Pero desarrollar un explosivo desde cero es, sin duda, algo complejo y peligroso que no está al alcance de todos. La baja intensidad de la explosión o los fallos en la activación del artefacto son factores que frustran atentados. Por esta razón, los movimientos extremistas ponen el énfasis en redactar instrucciones adaptadas a terroristas *amateurs* para que no sufran este problema, en un formato que recuerda a experimentos de ciencia en el ámbito escolar (Wiskind, 2016): los pasos a seguir están acompañados de imágenes y se incluye una lista de "ingredientes" simples que pueden conseguirse en ferreterías, tiendas de electrodomésticos o en un supermercado. Por supuesto, la calidad del artefacto seguirá siendo baja, pero intentar obtener los materiales necesarios para crear un explosivo más sofisticado, aunque no es imposible, aumenta el riesgo de detección y rompe con la lógica impermeable de la resistencia sin líderes.

Lo cierto es que algunos documentos, como el Manual del guerrillero urbano, exigen que antes de aprender a fabricar explosivos caseros el individuo ha de tener conocimientos de química y ser capaz de mantener unas condiciones de seguridad mínimas para evitar accidentes. A partir de aquí, la variedad de explosivos que pueden crearse es amplia. La tipología más básica se compone por las bombas de tubo o *pipe bombs*, popularizadas tras el artículo "*Make a bomb in the kitchen of your Mom*" incluido en *Inspire*. En el atentado de Boston, los hermanos Tsarnaev detonaron dos bombas -las cuales seguían una receta similar a la del artículo- contenidas en ollas a presión. Su interior estaba repleto de perdigones y clavos para causar daños por metralla (Wiskind, 2016). Adicionalmente, utilizaron bombas de este estilo -pero de menor intensidad- a modo de granadas de mano en su huida de la policía (*Boston Marathon Bombing Trial Jury Sees Pipe Bombs Tossed at Police*, 2015). En *How to Survive in the West* se ofrece un esquema para que estas bombas puedan ser acompañadas por sistemas de detonación a distancia mediante dos teléfonos móviles conectados. *Inspire* también ofrece instrucciones para transformar bombas de tubo en explosivos trampa ideales para cometer asesinatos selectivos: ocultas en libros, paquetes, detrás de puertas e incluso con un componente magnético para adherirlas debajo de un vehículo. Mediante un mecanismo sencillo, estos artefactos estallan cuando la víctima realiza un gesto o movimiento determinado. Una tipología más compleja que las bombas de tubo es la de los explosivos plásticos, pero que ha sido tratada y nuevamente *Inspire* incluye instrucciones paso a paso para crearlos. En 2009, Umar Farouk

Abdulmutallab, afiliado a Al Qaeda, ocultó un explosivo de este tipo en su ropa interior e intentó -sin éxito- detonarlo en un vuelo de Ámsterdam a Detroit (Alandete, 2011).

Más allá de crear explosivos funcionales, algunos manuales ofrecen consejos para superar los sistemas de seguridad de aeropuertos -detectores de metales, perros entrenados o escáneres de rayos X- sin que los artefactos sean detectados o incluso detallan los puntos débiles de edificios comunes para facilitar su demolición.

6.2. Uso de armas de fuego

El empleo de artefactos explosivos, aunque eficaz, se ha vuelto cada vez más problemático a medida que las autoridades han impuesto prohibiciones o un mayor control en la venta de materiales necesarios para su fabricación. En su manifiesto, Breivik ya advertía de que algunas guías para crear bombas disponibles en Internet eran inútiles debido a la dificultad o imposibilidad para adquirir los componentes que requerían.[23] Además, desarrollar explosivos puede ser peligroso para un terrorista *amateur*. Por esta razón, está cobrando importancia el uso de armas pequeñas y ligeras por parte del terrorismo: un tipo de atentado que produce un terror distinto al de una explosión, uno mucho más personal (*Paris Terror Arsenal: Kalashnikovs, Rocket Launcher and Grenades*, 2015).

En todo debate sobre las armas de fuego aparece Estados Unidos como país donde su adquisición legal es sumamente fácil, incluso para individuos radicalizados. Pero la amenaza también está presente en Europa, pese a su control más férreo, y no es nada despreciable. Los terroristas, ya sean individuos solitarios o células pequeñas, disponen de distintos métodos para hacerse con armas de fuego. La principal vía es el mercado negro. En varios manuales, como *How to survive in the west* o 2083 se hace mención a la necesidad de intentar establecer contacto con el crímen organizado[24] ya que este tiene acceso a armamento militar y munición en grandes cantidades desde la descomposición de la URSS y su venta de excedentes. Actualmente, su arsenal se nutre de la reventa ilegal, el robo de cargamentos, la falsificación de los certificados de destino o el soborno a funcionarios de aduanas (Almaraz Sánchez, 2022). Pero el mercado negro presenta inconvenientes: el coste para obtener las armas es superior, es inaccesible para individuos

[23] "*20 years ago you could easily just walk into grocery stores, garden centers and apothecaries and just buy most of these materials over the counter. It was possible to acquire materials to make 70-100 different types of explosives, while the number is now reduced to 10-20 types of explosives.*" (Breivik, 2011)

[24] Breivik incluso ofrece una clasificación de grupos criminales con un análisis de riesgos a la hora de establecer relaciones.

sin conexiones o experiencias previas y el riesgo de ser detectado por parte de las agencias de inteligencia es alto. En realidad, ninguno de los manuales analizados tiene en cuenta los métodos alternativos que resultan de mayor utilidad para un terrorista individual o un grupo reducido de individuos que desean conservar su anonimato: la *dark web*, la reconversión de réplicas inutilizadas o armas de fogueo, la impresión 3D,[25] o la compra de piezas individuales para su ensamblaje final -lo que se conoce como comercio "hormiga"- (*Ibid*). La fabricación de armas artesanales con materiales de bricolaje o fontanería también es un peligro -y para el terrorismo, una oportunidad- a tener en cuenta. Las armas "hechizas" son populares entre la delincuencia común de LATAM al ser mucho más rentables que el armamento original.[26] Se trata de una opción desesperada, pues son artefactos inestables y que pueden estallar en las manos del usuario en el momento del disparo, pero son fáciles de obtener y no están sometidas a ningún tipo de registro (Esparragoza, 2021). En 2016 un youtuber de Jaén fue detenido por publicar vídeos en los que explicaba paso a paso cómo fabricar armas de fuego de este tipo. Aunque fue absuelto debido a que no eran operativas (Jiménez, 2017), es una muestra de que también existe interés por instruir en su desarrollo. Una última opción mucho más arriesgada implica el robo de armas de fuego directamente de una comisaría poco protegida. En 2022 un menor logró infiltrarse a plena luz del día en el centro de la Policía Nacional de Canillas, en Madrid, y sustraer dos armas de fuego. El robo no fue descubierto hasta la detención del joven horas después debido a que deambulaba en público mostrando una de las armas (Lopez Fonseca, 2022). Esto demuestra que existen brechas de seguridad que pueden ser explotadas por un individuo radicalizado con cierta experiencia o con ayuda de un caballo de Troya

La obtención del arma es un primer paso, pero el principal objetivo es poder manejarla adecuadamente. En este punto, los manuales no ofrecen instrucciones de cómo usarlas pues directamente hacen referencia a *Youtube*, donde el contenido formativo en el ámbito de las armas de fuego es abundante y legal. En cambio, ofrecen consejos para poder obtener experiencia práctica sin tener que recurrir a campos de tiro registrados, lo que llamaría demasiado la atención, especialmente en Europa. En *How to survive in the west* se recomienda adquirir -antes de un arma de fuego real- armas de juguete, de *paintball* o *airsoft* o crear armas primitivas -ballestas, arcos y tirachinas caseros- para practicar puntería en el interior del domicilio o en el jardín. Obviamente esto no sustituye el

[25] Stephan Balliet, el terrorista individual que atacó una sinagoga en Halle, usó un arma impresa en 3D por él mismo (*El Neonazi De Halle Podría Haber Fabricado Sus Armas En Una Impresora 3D*, 2019).

[26] En España ciertos grupos criminales organizados también han recurrido a este medio barato. Durante el desmantelamiento de cinco plantaciones de marihuana en Segrià, se encontraron varias armas rudimentarias cargadas con cartuchos y colocadas a modo de trampas (*Una Banda De Narcos De La Marihuana Activa Un Parany per Disparar Contra Mossos Al Segrià*, 2021).

entrenamiento con un arma real ya que no refleja su peso o retroceso. Por su parte, Breivik en 2083 hace mención a campos de tiro ilegales ocultos en espacios interiores. También recomienda viajar a algún país africano de mayoría cristiana -dando a entender que los viajes a países islámicos alertan a los servicios de inteligencia- donde el control armamentístico sea deficiente. Por último, en el Manual del guerrillero urbano se recalca la importancia de cuidar las armas, repararlas e instalar un pequeño taller para ello, especialmente si se planea llevar a cabo una campaña de acciones terroristas más o menos prolongada.

6.3. Ejecución de un asalto

Un asalto es un ataque directo a un espacio o edificio con el objetivo de eliminar a todos los presentes. Las instrucciones referidas a ejecutar este tipo de atentado se centran en asaltos con armas de fuego y asaltos en los cuales el terrorista pretende escapar vivo. Es evidente que un asalto con armas blancas o un ataque suicida requiere de poca o nula preparación por su simpleza. Aunque sea una misión compleja, asaltar un lugar y huir es posible, de hecho es ideal para llevar a cabo múltiples atentados[27] y difundir un mensaje de miedo: que un terrorista ande suelto genera una gran repercusión mediática, aunque solo sea por unas horas. Tras el atentado contra la sede de *Charlie Hebdo*, los hermanos Kouachi se dieron a la fuga durante varios días, provocando la movilización de 3000 agentes de policía (Yárnoz, 2015). Meses después, en California, Syed Rizwan Farook planificó un tiroteo en su lugar de trabajo junto a su esposa Tashfeen Malik, dando muerte a 14 ex-compañeros. Los autores huyeron en coche mientras eran perseguidos por una veintena de agentes de policía, siendo abatidos horas después (*Los Autores Del Tiroteo De California Dejaron a Su Bebé a La Abuela*, 2017).

Los manuales que explican cómo llevar a cabo un asalto coinciden en la necesidad de una buena selección del objetivo y de la recolección de información acerca de este. Los objetivos deben ser lugares o edificios escasamente protegidos que ofrezcan la oportunidad de causar la mayor cantidad posible de daños colaterales: comisarías pequeñas, espacios religiosos, reuniones de partidos políticos, discotecas, lugares simbólicos o simplemente zonas frecuentemente aglomeradas. Tras esto es necesario investigar a fondo el lugar: entradas, salidas, horas de mayor confluencia, calles cercanas, seguridad existente, etc. Para ello puede ser empleada la observación en persona, fuentes abiertas y otros métodos

[27] Breivik explica que tras la comisión de un asalto el terrorista será detenido de forma inevitable. En lugar de desplazarse a un lugar seguro una vez finaliza el atentado para esperar a ser capturado, aconseja preparar de antemano un conjunto de objetivos y atacarlos sucesivamente.

ilegales que se verán en los próximos apartados -espionaje, interrogatorio, sobornos, brechas de seguridad informática o vigilancia con drones-. Se recomienda antes de ejecutar el asalto diseñar una estratagema para lograr un mayor impacto, por ejemplo, causar una explosión en un lugar distinto al del tiroteo para desviar la atención, hacerse con un traje que genere confusión -como hizo Breivik disfrazado de agente de policía- o infiltrarse previamente en el lugar objetivo.

El transcurso del asalto recibe mucha atención por parte de estos manuales. En el manual del guerrillero urbano se afirma que los asaltos implican combate y tiroteos a corta distancia, por lo que el terrorista debe actuar rápido, desplazarse con cautela y ahorrar munición. Si hay presencia de cuerpos de seguridad armados saber disparar el arma de fuego no es suficiente, pues se requiere de un mínimo conocimiento táctico para sobrevivir. En este sentido, en *How to survive in the west* se hace mención a la formación en técnicas MOUT (*Military operations in urban terrain*) para reaccionar adecuadamente en el combate urbano. En el caso de que haya múltiples terroristas ejecutando el ataque, estos deben poder coordinarse y actuar como un equipo o “grupo de fuego”, tal y como Marighella los define. Es posible que el terrorista individual o uno de los miembros de la célula haya resultado herido. Nuevamente, a menos que se trate de una actuación suicida o las circunstancias no permitan su tratamiento, en el manual del guerrillero urbano se menciona la importancia de tener conocimientos básicos en primeros auxilios, aplicables una vez se llegue a un lugar seguro.

El asalto debe ser de corta duración. Se han de evitar las batallas decisivas, el terrorista individual o las células han de hacer ataques breves para así generar un estado de tensión y huir. Lo más adecuado es escapar antes de que se aproximen un mayor número de cuerpos de seguridad, pero cabe la posibilidad de que los terroristas se vean rodeados. Por esta razón Breivik ofrece instrucciones para superar una barrera policial o evitar ser flanqueado. Independientemente de la brevedad del ataque, un plan de huida es necesario. Esto requiere de un conocimiento previo del terreno para convertirlo en un aliado, de ahí la importancia de una recolección de información sobre el objetivo. Saber cómo utilizar sus desniveles, sus alturas y sus puntos bajos, sus curvas, sus irregularidades, sus pasajes ocultos, sus calles abandonadas… Todo puede servir para despistar a los perseguidores y evitar un intento fallido de fuga por culpa de un callejón sin salida, una zona en obras imprevista o un embotellamiento de tráfico.

6.4. Asesinatos

El asesinato selectivo es un tipo de atentado que también ha recibido atención por parte del terrorismo moderno -a pesar de no generar el mismo impacto que los anteriores-, consecuentemente, también existen instrucciones para llevarlo a cabo. En realidad, estas son similares a las de un asalto ya que distinguen tres fases: preparación, ejecución y huida. La preparación implica la selección del objetivo y la recolección de información acerca de este. A diferencia de un asalto, se aconseja que la víctima no sea escogida al azar, sino que sea un individuo cuya muerte ofrezca ventajas estratégicas, tácticas o simbólicas para el movimiento extremista. El número 10 y 14 de la revista *Inspire* incluyen una lista titulada "*Wanted Dead or Alive for Crimes Against Islam*" para guiar al lector en la selección de objetivos. La lista está compuesta por políticos occidentales, dibujantes satíricos -entre los que se encontraba Stéphane Charbonnier, víctima del atentado a *Charlie Hebdo*- y personalidades económicas como Bill Gates. En *Dabiq,* el Estado Islámico también ofrece una lista de víctimas, pero se centra en líderes musulmanes "apóstatas", como el ayatolá Jamenei o Tayyip Erdogan (Wiskind, 2016). Por su parte, Breivik también elabora una categoría de "traidores" -líderes políticos que apoyan la islamización europea, miembros de ONGs, profesores o periodistas- con diferentes grados de prioridad. Sin embargo él mismo advierte que ciertos objetivos son inalcanzables para un terrorista individual o una célula pequeña, por lo que en vez de planificar su asesinato y fracasar en el intento es mejor dedicar los esfuerzos a víctimas menos protegidas. Una vez escogida la víctima empieza la obtención de información, nuevamente a través de la observación, fuentes abiertas -especialmente mediante publicaciones en redes sociales- o métodos ilegales. Según los manuales, gran parte del esfuerzo destinado a una operación de asesinato debe corresponder a esta fase. Lugar de residencia, lugar de trabajo, lugares de ocio frecuentados, horarios, rutas de transporte, familiares y amistades… Se insiste en que todos estos datos pueden ser de utilidad para detectar vulnerabilidades y desarrollar un plan de ejecución.

El plan de ejecución debe contemplar el lugar del asesinato, el arma empleada y la forma de acercamiento a la víctima. Evidentemente, el lugar ideal es aquel en el que hay menos testigos y la víctima cuenta con menor protección. Respecto al método, el terrorista puede recurrir a un arma de fuego, explosivos trampa, un arma blanca -para lo cual se recomienda entrenamiento cuerpo a cuerpo- o veneno -ciertos manuales explican cómo preparar ricina o ántrax-. El acercamiento a la víctima es vital y ha de contemplar formas de infiltrarse en un edificio sin ser descubierto, vías a través de las cuales hacer llegar el explosivo o veneno, tapaderas e incluso disfraces.

Por último, se debe preparar un plan de huida, como si se tratara de un asalto. Pero en lugar de alertar a las FCS desde un primer momento, en la revista *Inspire* se recomienda aprender a eliminar todas los pruebas y rastros en la escena del asesinato que demuestren la participación del terrorista. De esta manera se puede conseguir un tiempo valioso para ejecutar más ataques antes de ser detenido.

6.5. "Ultimate Mowing Machine"

El atentado del 17 de agosto en las ramblas de Barcelona o el de Niza en 2016 demuestran que un vehículo de grandes dimensiones circulando por una zona aglomerada y arrollando a los civiles que encuentra a su paso puede causar un daño enorme. Este tipo de ataque, contemplado en la revista *Inspire*, está diseñado para convertir cualquier vehículo "en una máquina de segar a los enemigos de Alá" (Wiskind, 2016). Se trata de un ataque simple que no requiere de apenas recursos ni tampoco formación. Sin embargo, la revista sugiere perfeccionarlo a través de una planificación -de la ruta y la hora- y mediante la modificación del vehículo, ya sea reforzando su estructura o colocando cuchillas a su alrededor. Es aquí donde las instrucciones se hacen necesarias al entrar en juego conocimientos mecánicos.

6.6. Empleo de drones como arma terrorista

El uso de VANT (Vehículos Aéreos no Tripulados) gana cada vez más peso en el ámbito bélico, como se ha podido observar recientemente en el conflicto ucraniano. Pero las mismas funcionalidades que convierten a los drones en instrumentos ideales para el campo de batalla también resultan de utilidad para el terrorismo. Sin embargo, los sofisticados VANT empleados por los ejércitos modernos no están al alcance de la gran mayoría de grupos terroristas. Además, en el hipotético caso de que consiguieran uno, su tamaño y firma radar restringen el vuelo a zonas donde el grupo disfrutara de superioridad aérea, como ciertos Estados fallidos. Por esta razón, la atención debe ponerse sobre los VANT de tipo comercial o uso civil en manos de terroristas: una amenaza realista y muy susceptible de afectar a Occidente. Los VANT comerciales pueden ser adquiridos fácilmente a través de Internet y muchos no requieren de licencia. Su relativo bajo coste permite que sean herramientas asequibles para células pequeñas o terroristas individuales. Además, un dron es un bien de doble uso difícil de regular al tener finalidades civiles o recreativas, por lo que su prohibición sería percibida como excesiva e injustificada.

Ligando esto con el objeto de la investigación, ¿qué necesidad formativa existe respecto a los drones por parte del terrorismo? En realidad el entrenamiento necesario para pilotar un

VANT comercial es bajo ya que cuentan con sistemas que los hacen gobernables incluso para usuarios inexpertos, como navegación por satélite, piloto automático, o sensores anticolisión (Marín Delgado, 2018). La habilidad requerida actualmente consiste en poder transformar a estas máquinas de naturaleza inofensiva en armas letales y polivalentes, además de poder usarlas efectivamente como tal. Aunque estos drones suelen equiparse con cámaras para captar imágenes y vídeos a tiempo real -lo que puede ser especialmente útil para las fases de reconocimiento y vigilancia en otro tipo de atentados- existe el interés de poder modificarlos y armarlos para que dejen de ser meros ojos en el aire. De hecho, ya se han producido atentados -fallidos- de este tipo. Por ejemplo, en 2012 tres individuos supuestamente asociados a Al Qaeda fueron detenidos antes de que pudieran ejecutar un ataque en el centro comercial Puerta Europa, en Algeciras. En la vivienda donde residían dos de ellos se incautaron un avión de aeromodelismo con capacidad de carga de 1 kilo, explosivos y material videográfico que mostraba un aeromodelo dejando caer un fardo (*Los Terroristas Iban a Atentar En El Centro Comercial Puerta De Europa*, 2012). Posteriormente, en 2014, El Mehdi Semlali Fahti, marroquí residente en Estados Unidos, planificó un ataque contra la universidad de Harvard y un edificio federal con un dron de juguete que pretendía usar como una bomba (*Moroccan Sentenced to 2 Years for 'Plotting' to Attack Harvard University*, 2014).

El Estado Islámico ya ha distribuido por Internet manuales y guías para instruir a individuos sin conocimiento en la conversión de drones en vectores de ataque (Marín Delgado, 2018). Tales documentos se centran en equipar a VANT con explosivos, cohetes rudimentarios o convertirlos en drones "kamikaze", como ha estado haciendo Estado Islámico en Siria o Irak. Pero lo cierto es que el avance tecnológico tolera cada vez más combinaciones. En el futuro podrían proliferar instrucciones para equipar drones con armas improvisadas -cuchillos, dardos o bolas de hierro-, armas de fuego, armas incendiarias o incluso sistemas de fumigación para dispersar agentes químicos o bacteriológicos, como ántrax (*Ibid*). Aunque los drones más accesibles tienen una limitada capacidad de carga -y por lo tanto su letalidad es menor- resultan de especial utilidad para cumplir el objetivo del terrorismo: difundir un mensaje de pánico. El simple hecho de que estos atentados puedan producirse en cualquier lugar y a cualquier hora genera inseguridad y tensión, especialmente si los drones son utilizados a modo de enjambre.

6.7. Ciberterrorismo

El plano virtual o digital, es decir, las nuevas tecnologías, se han convertido en un nuevo campo de batalla donde los terroristas ven una oportunidad excelente para internacionalizar

sus operaciones. Si se hace un símil con las categorías de ciber delitos de David Wall (2014), actualmente prevalecen las actividades terroristas en la red consideradas como "delitos dentro de la máquina": financiación, difusión de propaganda extremista, adiestramiento, reclutamiento, comunicación interna o la planificación. Pero no se debe descartar la posibilidad de que los grupos terroristas dejen de percibir Internet como un simple medio y empiecen a considerarlo como un espacio ideal en el que ejecutar ciberataques o "delitos contra la máquina". El ciberterrorismo apenas es tratado por los manuales estudiados -la mayoría fueron redactados antes de la extensión a gran escala de Internet- a excepción de *How to survive in the west*, que brevemente menciona la posibilidad de practicar el *hacking* y el *phishing* como vía de financiación. Sin embargo, es conveniente incluirlo como una nueva necesidad formativa que aún se sitúa en una fase temprana en comparación a habilidades tradicionales, como la fabricación de explosivos. Se dice que las amenazas son el resultado de la suma o intersección de tres conceptos: intención, capacidad y oportunidad (*Defensa Activa E Inteligencia: Threat Intelligence En Los Entornos Industriales*, 2018). En el caso de la amenaza del ciberterrorismo, la intención de los diferentes movimientos extremistas de llevar a cabo ataques virtuales con mayor frecuencia parece no estar desarrollada aún. En cambio, existen capacidades para hacerlo: en la *darknet* proliferan los criminales dedicados a crear programas maliciosos y a distribuirlos como si fueran armas de fuego en el mercado negro. Estos individuos con conocimientos en informática también organizan "cursillos" de pago para instruir a usuarios en el *hacking* ilegal (Assolini, 2012). Respecto a las oportunidades, lo cierto es que la ciberseguridad es un tema en boca de todos, pero que a menudo no recibe la suficiente atención. La ciudadanía está poco concienciada sobre los peligros en la red y olvida tomar precauciones para protegerse, pero es un problema que va más allá de la gente corriente. A nivel empresarial se sobreestiman los conocimientos en ciberseguridad y, según Kaspersky, la gran mayoría de empleados requiere mejorar sus habilidades básicas de autoprotección virtual (*Nine Out of Ten Employees Need Basic Cybersecurity Skills Training*, 2022).

El ciberterrorismo puede perseguir tres finalidades: financiación, espionaje y disrupción. Por una parte, los terroristas pueden seguir el mismo rumbo que la ciberdelincuencia y utilizar las nuevas tecnologías para financiarse a través de troyanos bancarios, *ransomware* o mediante la simple pero eficaz ingeniería social -*phishing*-. Por otra parte, pueden recurrir a *spyware* o a ataques *Man in The Middle* para interceptar comunicaciones y obtener información privada del dispositivo de sus víctimas, lo que puede ser especialmente útil para planificar un atentado. Por último, también existe la posibilidad de un ciberataque cuya única finalidad sea la disrupción, como si de un atentado se tratara. Ataques de denegación de servicio, DDoS, virus, gusanos informáticos y otro tipo de *malware* provocan daños que van

más allá del dispositivo. En la actualidad, el plano virtual y físico se unen gracias a la *datafication*, el *machine learning*, los algoritmos, el *Internet of Things* y un conjunto de avances integrados en una amplia variedad de sectores. Como consecuencia, un ciberataque podría causar daños patrimoniales, económicos, pérdidas humanas y mermar la confianza ciudadana en las autoridades (Schrijvers et al., 2021, 4). Además, las políticas de ciberseguridad nacionales suelen centrarse en la mitigación y la prevención, pero incluyen pocas o nulas previsiones para reaccionar cuando efectivamente se da un ciberataque, es decir, la preparación ante una situación de emergencia causada por una disrupción digital es deficiente (Papakonstantinou, 2022). De hecho, políticos estadounidenses han alertado de que un ciberataque con finalidad disruptora tendría consecuencias tan graves como el 11-S. Algunos incluso han apuntado que podrían verse afectadas las infraestructuras críticas, como las centrales nucleares. Fernández Nieto (2018) afirma que tal situación no se ha dado hasta la fecha sencillamente porque los terroristas no cuentan con un ciberarma capaz de comprometer la seguridad de una infraestructura crítica. Las ciberarmas más sofisticadas, como *Stuxnet*,[28] pertenecen exclusivamente a los Estados con capacidades de ciberguerra. A menos que un Estado ofrezca a un grupo terrorista un ciberarma, los terroristas deberán superar enormes barreras económicas, científicas y tecnológicas para desarrollar una por su cuenta.

En realidad, la lógica de la resistencia sin líderes sigue siendo aplicable en el ciberterrorismo. El riesgo de ser detectado durante el intento de atacar una infraestructura crítica o un edificio gubernamental principal es alto y no es adecuado asumirlo. Por el contrario, resulta más conveniente enfocarse en objetivos sencillos con un grado de ciberseguridad baja: particulares, edificios administrativos, hospitales, comisarías pequeñas, empresas industriales, etc.

6.8. Estrategias para evitar la detección

Como ya vimos, la lógica fundamental de la resistencia sin líderes, ya sea individual o en forma de células pequeñas, es el aislamiento, la independencia y la impermeabilidad. El terrorista que “sobrevive” y planifica ataques dentro de la sociedad que precisamente pretende destruir debe de hacerlo con sumo cuidado ya que no cuenta con la misma libertad que un terrorista de Afganistán, Siria o Irak. De hecho, el terrorista de Occidente se enfrenta a un Estado fuerte con servicios de inteligencia plenamente operativos y a la búsqueda de cualquier señal débil, indicador o prueba de su radicalización. Sin embargo, a

[28] Gusano informático descubierto en 2010 que fue empleado para retrasar el proyecto nuclear iraní. De origen desconocido, se cree que fue desarrollado conjuntamente por Estados Unidos e Israel.

menudo los terroristas imprudentes o con poca experiencia cometen errores y dejan tras de sí un rastro fácilmente detectable, lo que conlleva su detención antes incluso de que cometan un atentado. Por esta razón todos los manuales anteriormente listados dedican apartados a hablar de la importancia de pasar desapercibido al mismo tiempo que se contribuye a la lucha por la narrativa extremista violenta. En *Al Qaeda Handbook* se ofrece abundante información al respecto en un estilo que recuerda a un manual diseñado para agentes encubiertos.

Algunas de sus instrucciones están especialmente dirigidas a yihadistas que hayan viajado a Occidente desde el extranjero y deban empezar de cero en territorio hostil. Ahora bien, también pueden beneficiar a terroristas autóctonos ya "integrados" en Occidente. Esto puede verse en la existencia de instrucciones referidas a la selección de un piso franco adecuado, métodos de financiación -legales e ilegales- y la creación de múltiples identidades. Tanto el terrorista extranjero como autóctono deben mostrar una cara compatible con el lugar en el que operan y no revelar sus aspiraciones. Esto incluye la capacidad contemplada por el Corán conocida como *taqiyya*, que excepcionalmente permite al yihadista actuar como un camaleón y ocultar sus costumbres islámicas para confundir a sus enemigos. Beber alcohol, afeitarse la barba, usar ropa occidental, limitar el rezo a lugares privados o evitar criticar conductas contrarias al islam por parte de otras personas (Yitzhak, 2019). Tom Metzger también propuso un equivalente neonazi a la *taqiyya*, afirmando que los individuos afines a esta ideología deben vivir en el "underground político" y comportarse como ciudadanos corrientes (Arias Gil, 2018). Más allá de esto, para evitar despertar sospechas el terrorista ha de saber desempeñar el rol de uno o más personajes ficticios que justifiquen el trabajo con ciertos materiales -para la fabricación de armas o explosivos-, la recepción de visitas -por parte de miembros de la célula- u horas de aislamiento dedicadas secretamente a la planificación de un atentado. Para ello deben interiorizarse sus nombres, empleos y trasfondos falsos. Además, se ofrecen instrucciones para preparar tapaderas acordes a las identidades. El manual explica que en el puesto fronterizo o aeropuerto el terrorista procedente del extranjero podría ser sometido a preguntas de seguridad relacionadas con los motivos de su viaje, métodos para costearlo, la duración de su estancia o conocidos a los que visitará. Aunque no se trata de un interrogatorio policial, es necesario ensayar las respuestas a estas preguntas típicas para que concuerden con la identidad escogida. Lo mismo sucedería si el terrorista tuviera que atravesar una zona reservada durante una misión o fuera cuestionada su presencia en algún lugar por un agente de policía. Por ejemplo, en *How to survive in the west* se aconseja recurrir a una tapadera simple: cuando el terrorista es descubierto manipulando un

vehículo o portando algún objeto sospechoso puede argumentar que se trata de una broma con cámara oculta.

La falsificación de documentos de identidad y los pasaportes también es una habilidad necesaria para dotar de más credibilidad a las múltiples identidades creadas. Sin embargo, a día de hoy es casi imposible de adquirir para alguien sin recursos y conocimientos previos.[29] Por su parte la falsificación de otro tipo de documentos no oficiales sigue siendo posible pero las circunstancias obligan a una actualización. Marighella creía vitales en un guerrillero la capacidad de confección de sellos falsos, el dominio de la técnica de la caligrafía, la imitación de firmas y la imitación de documentos escritos a mano. Es evidente que la digitalización ha causado un abandono progresivo del papel, por lo que la falsificación será de documentos y correos electrónicos.

Cuando haya logrado engañar a la población civil sobre sus verdaderas intenciones el terrorista debe ser cauteloso y evitar que, en el caso de estar siendo monitorizado por un servicio de inteligencia, este obtenga cualquier tipo de prueba incriminatoria. Para ello ha de tomar precauciones en cierta medida similares a la contrainteligencia. En principio un terrorista individual no se verá afectado ya que si mantiene su impermeabilidad y aislamiento no puede despertar ningún tipo de atención, aunque puede recurrir a tales precauciones para mejorar su propia seguridad. Por el contrario, la contrainteligencia tiene un valor vital para células pequeñas cuyos miembros desean comunicarse entre sí sin poner en riesgo su identidad. En este sentido, son las comunicaciones en persona las más riesgosas y las que reciben mayor atención del manual. Las instrucciones abarcan la selección de un lugar adecuado para la reunión, la creación de gestos para identificar a los miembros, la búsqueda de ubicaciones alternativas en caso de que exista vigilancia y el comportamiento durante la reunión. Incluso se habla de la importancia de planificar una ruta de escape en caso de que las FCS se aproximen al punto de encuentro y, si la reunión se ha llevado a cabo en un domicilio, de preparar escondites para ocultar documentos, armas u objetos relevantes. El desplazamiento hacia la ubicación de la reunión también es tenido en cuenta: se utilice transporte público o privado se dan explicaciones para poder determinar si uno está siendo observado y para evitar ser seguido. En lo que se refiere a las

[29] La fecha del *Al Qaeda Handbook* es desconocida pero claramente es anterior al avance tecnológico del siglo XXI. Actualmente la falsificación de documentos de identidad o de pasaportes resulta mucho más compleja, especialmente para individuos inexpertos o con pocos recursos. Esto ha empujado a ciertos grupos criminales a especializarse en la falsificación de documentos oficiales y a distribuirlos en el mercado negro con precio variable en función de su calidad. También ha podido observarse el robo de documentos reales para posteriormente suplantar a la persona afectada (Ballesteros, 2020). Esta oferta hace que sea más probable que los terroristas recurran al mercado negro en lugar de “aprender” a falsificar.

comunicaciones telefónicas, el manual insiste en la importancia de crear códigos, contraseñas o escoger palabras con doble sentido para que el verdadero significado de la conversación no sea descubierto, lo que también debe hacerse en la comunicación escrita. También aconseja verificar si el dispositivo está siendo monitorizado[30] y aprender los números de teléfono de memoria, sin dejar registro de estos. Por otra parte, las comunicaciones en línea no son contempladas en *Al Qaeda Handbook* pero sí en *How to survive in the west*, donde se explica la necesidad de utilizar la red TOR para ocultar la IP del usuario.

6.9. Obtención de información y espionaje

Disponer de información actualizada sobre el enemigo o un objetivo en concreto es sumamente importante tal y como se ha visto en las necesidades formativas anteriores. Conocer sus intenciones, fortalezas y debilidades permite al terrorista diseñar un plan de ataque y determinar la mejor forma para mantener su propia seguridad. La inteligencia de fuentes abiertas (OSINT) es mencionada en *Al Qaeda Handbook* como el principal método de recolección de datos. Periódicos, revistas, libros, noticias emitidas por televisión, publicaciones en redes sociales, opiniones y comentarios de los ciudadanos… Las fuentes abiertas no exponen al terrorista a ningún tipo de peligro y aportan un gran volumen de información, pero a menudo se trata de información común. Por ello el manual dedica mayor atención a los métodos ilegales o encubiertos de inteligencia: fuentes de diversa naturaleza que aportan información confidencial. Estas fuentes dan acceso, por una parte, a datos sensibles relacionados con personal del gobierno, policías, militares y personalidades importantes -lugar de residencia, lugar de trabajo, lugares frecuentados, horarios, familiares y amigos-. Por otra parte, pueden ayudar a detectar fortalezas y debilidades en edificios estratégicos, comisarías o bases militares. Sin embargo los métodos ilegales generan un riesgo para el terrorista si no se explotan adecuadamente, de ahí que existan instrucciones detalladas para evitar hacer saltar las alarmas.

Al Qaeda Handbook explica paso a paso cómo llevar a cabo de forma segura el seguimiento y vigilancia de un individuo, ya sea a pié o en vehículo. Al mismo tiempo, tal y como se vio en el apartado anterior, se ofrecen técnicas para determinar si el propio terrorista está siendo observado. La descripción de edificios o lugares también es tenida en cuenta y abarca las formas más eficaces para fotografiar o dibujar el objetivo y qué

[30] La desinformación también forma parte de la contrainteligencia. En el caso de que el dispositivo esté siendo monitorizado se recomienda aprovechar la situación para comunicar información falsa y confundir a las agencias de inteligencia.

características se deberían destacar. El robo de documentos es otra fuente ilegal clásica, pero actualmente la sustracción de documentos relevantes o la interceptación de comunicaciones se ejecutan en el plano virtual, por lo que la formación en ciberataques ya comentada es necesaria. Quizá lo que despierta un mayor interés es la utilización de individuos cercanos a los objetivos o que trabajen en los edificios seleccionados (HUMINT). El reclutamiento de agentes dobles o caballos de Troya a través de la coacción, el soborno o la persuasión es útil ya que ofrece información de primera mano, pero puede convertirse en un arma de doble filo si el agente trata de engañar al terrorista. Por ello, nuevamente se ofrecen una serie de precauciones a seguir, no sólo para seleccionar al agente adecuado, sino también para garantizar su lealtad. En la disciplina HUMINT se incluyen diferentes métodos de interrogatorio y tortura, pero previamente el individuo en cuestión debe ser secuestrado. El manual del secuestro[31] de Abdel Aziz Al Muqrin explica cómo seleccionar un objetivo, cómo capturarlo y cómo tratarlo una vez esté en poder del terrorista.

6.10. Counter Interrogation Tactics

Eventualmente el terrorista podría llegar a ser detectado por un servicio de inteligencia y capturado para su interrogatorio. A menos que la participación del individuo o individuos en un atentado sea evidente, el interrogatorio tiene por objetivo recopilar pruebas que demuestren sus destructivas aspiraciones. En este caso, el interrogatorio es una fase importante ya que la libertad o encarcelamiento del terrorista depende de su habilidad para no revelar información, por insignificante que parezca, que pueda incriminarlo. Por esta razón los terroristas capturados suelen emplear técnicas anti interrogatorio. Se trata de estrategias adoptadas por los sospechosos para evitar cooperar con el personal policial o militar encargado del interrogatorio. Tales estrategias pueden ser adquiridas a través de instrucciones y entrenamiento proporcionado por un movimiento extremista (Alison et al., 2014). El *Green Book* del IRA y la lección número 17 del *Al Qaeda Handbook* coinciden en la importancia de mantener silencio total durante el interrogatorio. El mismo título que da comienzo al *Green Book*, "*Whatever you say, say nothing*", es explícito en esta idea. Sin embargo, el silencio no es el único método recurrido. El estudio de Alison et al. (2014) de 181 entrevistas policiales a terroristas convictos ha permitido identificar 9 tipos de técnicas anti interrogatorio comunes en yihadistas e individuos de extrema derecha: cambiar el tema discutido con uno no relacionado, aportar información ya conocida, retractar una afirmación -o negar que hubiera sido realizada en un primer momento-, negarse a hacer comentarios,

[31] Más allá de la obtención de información, el secuestro también puede ser un método de financiación o estar acompañado del asesinato. La filmación y difusión de la muerte de la víctima genera el clima de miedo que precisamente el terrorismo persigue.

evitar mirar a los interrogadores, permanecer en silencio absoluto, ofrecer una respuesta improvisada, dar respuestas monosilábicas y declarar una falta de memoria. Al mismo tiempo, estas conductas pueden agruparse en cinco ramas. La primera, referida a las conductas verbales -incluye los cambios de tema, la aportación de información ya conocida o dar respuestas improvisadas- pretende confundir a los interrogadores y aparentar cooperación. La segunda, referida a las conductas pasivo verbales -dar respuestas monosilábicas o declarar falta de memoria- trata, nuevamente, de aparentar cooperación, pero de forma mucho más limitada. La tercera, referida a las conductas pasivas -incluye evitar el contacto visual con los interrogadores y permanecer en completo silencio- son una forma de distanciarse psicológicamente de la situación. La declaración de "sin comentarios" y las retracciones ocupan dos ramas independientes y suponen un intento de entorpecer e interrumpir el flujo de la interrogación.

Más allá de las técnicas anti interrogatorio, el *Green Book* trata de preparar mentalmente a los miembros del IRA ante situaciones de estrés como una detención y un interrogatorio. Se explican las supuestas técnicas empleadas por las FCS para quebrar la voluntad del terrorista, para generarle culpa, miedo y desconfianza entre sus aliados. Según este manual, los interrogadores revelarán todos los datos íntimos del sospechoso, gritarán, amenazarán, harán intentos de persuasión, engañarán, torturarán -física y psicológicamente- y humillarán. Se insiste en evitar caer en estas técnicas ya que al dar resultados los interrogadores se verán incentivados para aplicarlas con más intensidad. En realidad, el manual pretende hacer ver al lector que tales métodos de interrogatorio son un intento desesperado de obtener información y que, si se aguanta el tiempo suficiente, el individuo deberá ser liberado por falta de pruebas. Para ello se hace mención a la importancia de ignorar a los interrogadores y se ofrecen consejos para dirigir la atención a otra parte en un intento de distanciarse psicológicamente de la situación.

En el caso de que se obtengan pruebas y el terrorista finalmente sea llevado a juicio, lo único que puede hacer es intentar entorpecer el proceso y causar confusión. En *Al Qaeda Handbook* se aconseja denunciar el sufrimiento de malos tratos y torturas por parte de los interrogadores, lo que obligará a retrasar las investigaciones. Por otra parte, el terrorista también puede proclamar que no es el único con sus mismas aspiraciones y que hay más individuos agrupados, de forma similar a la declaración de Breivik y el supuesto grupo de "Los Caballeros Templarios de Europa" (Holden, 2011).

7. Escenario futuro: Videojuegos formativos de contenido terrorista

En este apartado final se presentarán ejemplos de cómo el terrorismo podría beneficiarse de los videojuegos en lo que se refiere a la formación y el entrenamiento. Dado que no hay casos documentados de videojuegos formativos empleados por terroristas ni tampoco existe bibliografía al respecto, en todo momento se describirán videojuegos ficticios que en un hipotético futuro podrían -o no- desarrollarse. Estos han sido ideados en base a la combinación de las necesidades formativas que el terrorismo pretende satisfacer y el estado actual / futuro de los *serious games*. En otras palabras, los *serious games* utilizados por actores legítimos en el ámbito militar o policial y que fueron analizados anteriormente han sido reimaginados para adaptarlos al contexto del terrorismo.

7.1. Fabricación de explosivos

Dado que la fabricación de explosivos es una habilidad que requiere de conocimientos técnicos y práctica para su desarrollo, en un futuro no sería extraño que proliferen simuladores que reflejen su proceso paso a paso. En realidad, es una vía de entrenamiento mucho más eficaz que los manuales. En estos documentos se listan los materiales necesarios y las instrucciones para construir el artefacto, a menudo acompañadas de imágenes para facilitar el aprendizaje. Sin embargo, estas instrucciones se han de llevar a cabo en la vida real, lo que genera riesgos e inconvenientes. Al tratar con materiales que, combinados, suponen una fuente de peligro, cualquier fallo a la hora de seguir las instrucciones puede ser fatal para el terrorista. De hecho, aunque el artefacto no estalle prematuramente puede quedar inutilizado, lo que obligaría al terrorista a obtener nuevamente los materiales. Si bien estos explosivos improvisados están compuestos por materiales cotidianos, su compra reiterada puede despertar sospechas. Como consecuencia, el terrorista *amateur* tiene poco margen de error para experimentar con diferentes materiales o cargas explosivas. Por el contrario, los videojuegos ofrecerían la oportunidad de repetir este mismo proceso una y otra vez, sin riesgo de explosión ni coste alguno.

En este sentido, ¿qué tipo de *serious games* podrían desarrollarse con este fin? Sin duda, los simuladores avanzados / de alta fidelidad y la tecnología VR serían idóneos. Por una parte, encontramos simuladores basados en la esencia de *DIY Simulator* o *The Workshop Game*, donde el usuario tiene a su disposición maquinaria y herramientas diversas, pero en vez de producir piezas u objetos para el hogar… Debería fabricar explosivos plásticos, bombas de tubo, granadas caseras o bombas trampa. Omitiendo el conocimiento teórico

-este puede ser adquirido a través de los manuales clásicos- el aprendizaje en este tipo de simuladores se haría progresivamente al mismo tiempo que el usuario fabrica un explosivo. Un conjunto de niveles divididos por dificultad sería la clave de este progreso, siendo los primeros una introducción a los controles básicos -mostrando instrucciones para cada paso- y los últimos un "examen" cronometrado donde el usuario tiene por misión construir un explosivo avanzado sin ningún tipo de guía. También podrían incluirse niveles donde el usuario, más allá de construir el explosivo, debiera probarlo en una infraestructura o en un atentado. De esta forma se ofrecería un *feedback* doble, uno referido al potencial destructivo del explosivo y otro relacionado con la habilidad del terrorista para colocar el artefacto en una ubicación donde sea susceptible de causar más daños. Para ello, los motores *EXODUS* y *SMARTFIRE* -utilizados en AUGGMED pero adaptables al nuevo simulador- representarían adecuadamente los efectos de la explosión en el entorno y las víctimas. La tecnología 3D y los gráficos realistas permitirían reflejar hasta el más mínimo detalle de todo el proceso, desde la preparación de los materiales hasta el ensamblaje del artefacto. Por supuesto, el usuario podría interactuar mediante el ratón con cada elemento y una manipulación incorrecta conllevaría el fin del juego.

Por otra parte, la tecnología VR sería una evolución perfeccionada de todo lo anterior. No solo ofrecería una experiencia más inmersiva, sino que en el caso de complementarse con guantes de realidad virtual el usuario podría crear una bomba tal y como si lo hiciera en la vida real. Aunque los simuladores avanzados toleran un alto grado de interacción, esta no es una interacción natural. En cambio, los guantes hápticos hacen que los movimientos manuales sean reflejados totalmente. Por lo tanto, el usuario se vería obligado a tener control de su pulso, precisión y la presión que hace con sus dedos sobre los componentes, aspectos relevantes a la hora de fabricar explosivos. Por último, en el marco de la tecnología VR -pero fuera del contexto de los *serious games*- merece atención el peligro de la *holoportation* a través de la realidad aumentada. Esto podría facilitar que los terroristas individuales tengan un "entrenador personal" en su propio domicilio. Tan solo basta con imaginar la siguiente situación: un terrorista *amateur* residente en Europa coloca los materiales necesarios para fabricar un explosivo sobre su escritorio, pero en lugar de leer un manual opta por activar sus gafas inteligentes, las cuales comienzan a proyectar la imagen 3D de un terrorista veterano residente en Oriente Medio, quien también cuenta con esta tecnología. La proyección del veterano se posiciona al lado del *amateur* y, paso a paso, comienza a explicar el proceso de construcción del explosivo y a ofrecer *feedback* inmediato como si estuviera allí mismo.

7.2. Uso de armas de fuego

El uso de armas de fuego es una de las necesidades formativas que mejor se adapta a la instrucción mediante *serious games*, aunque no resulte barata. Gracias a la realidad virtual, los consejos ofrecidos por los manuales, como viajar a Estados con una regulación deficiente en la materia, asistir a campos de tiro clandestinos o utilizar armas de *paintball* y *airsoft* dejan de ser la única forma para obtener experiencia práctica sin despertar sospechas. Tanto la realidad virtual no inmersiva como la inmersiva permiten crear galerías de tiro donde el usuario puede abrir fuego con sus propias manos. Por una parte, los simuladores de tiro no inmersivos, como el simulador VIRTRA, recurren a réplicas físicas que al ser disparadas emiten una señal, algunas pueden incluso simular el retroceso del arma original. Por otra parte, los simuladores de tiro inmersivos permiten crear diferentes modelos virtuales de armas cuyo peso, retroceso y tacto puede sentirse en caso de ser empuñadas con guantes de realidad virtual y trajes hápticos. Esto elimina la necesidad de disponer de una réplica física para cada arma que se desee probar. La realidad aumentada también ofrece una propuesta interesante en lo que se refiere a la práctica de tiro, como en *URBAN*, donde el usuario empuña un arma de *airsoft* para abrir fuego contra imágenes proyectadas sobre dianas inteligentes capaces de registrar los impactos. Sin embargo, la realidad aumentada se centra en la precisión, y no en el manejo de un arma “realista”.

Estas opciones resultan de gran utilidad para el terrorismo, de hecho, ni siquiera sería necesario reimaginar los simuladores ya existentes para adaptarlos a sus necesidades, puesto que ya las satisfacen a la perfección. Pese a ello, podrían incluir pequeñas modificaciones de tipo visual: en lugar de mostrar dianas “neutras” en una galería de tiro inanimada, estas podrían representar a civiles o agentes de policía en un escenario típico de un atentado. De esta forma, se fomentaría la desensibilización del usuario -actuando como terrorista- y se facilitaría el aprendizaje de estímulos violentos.

Por otra parte, en el contexto de las armas de fuego también podrían proliferar simuladores de alta fidelidad destinados a terroristas con intención de adquirir conocimientos en torno al cuidado y mantenimiento de las armas, como en *Gunsmith Simulator*. Nuevamente, apenas se requerirían modificaciones respecto del simulador original ya que este permite estudiar e interactuar con los elementos de una gran cantidad de armas, todas diseñadas de forma realista en base a sus modelos de referencia. Pese a ello, estos simuladores podrían incluir contenido adicional orientado a la fabricación ilegal de armas de fuego. De forma similar a *DIY Simulator* o *The Workshop Game*, el usuario tendría a su disposición un conjunto de planos. En función del escogido, deberá crear un arma “hechiza” a partir de materiales

cotidianos, reconvertir réplicas inutilizadas / armas de fogueo o ensamblar piezas individuales. El simulador, más allá de ofrecer los pasos necesarios, también incluiría un sistema de *feedback* en base a la fiabilidad del arma creada.

7.3. Ejecución de un asalto

Durante un asalto, es muy posible que el terrorista individual o la célula deban enfrentarse a otros individuos armados dispuestos a detenerles. Para evitar el fracaso, la instrucción en técnicas MOUT (*Military Operations in Urban Terrain*) es necesaria. Existe una gran cantidad de manuales militares que ofrecen información e imágenes para actuar adecuadamente en situaciones de combate urbano, caracterizadas por la verticalidad, la multiplicidad de rutas y coberturas y el limitado campo visual. Pero las tácticas no se limitan a la teoría, deben ponerse en práctica en escenarios habilitados para interiorizarse, algo imposible para los terroristas en Occidente. Nuevamente, los *serious games* ofrecen una solución perfecta a estos obstáculos ya que han sido empleados para entrenamiento táctico de diferentes formas.

Por una parte, la opción más simple -y barata- sería un *serious game* básico como *Door Kickers: Simulations & Training* o *Close Combat Marine* reimaginado al contexto de un atentado. En lugar de dar órdenes a un grupo SWAT o un pelotón de marines, el jugador debería controlar con su ratón a un “grupo de fuego” formado por varios terroristas o un único terrorista individual. Reemplazando los escenarios típicos del ámbito policial / militar por niveles que representen a objetivos terroristas atractivos -centros comerciales, aeropuertos, calles abarrotadas, etc.- este tipo de juego obligaría al usuario a cumplir diferentes tareas al mismo tiempo que dirige a los terroristas a una zona determinada del mapa, lo que representa la huida. No alcanzarla antes de que se agote el tiempo supondría el fracaso. El jugador podría aprender nociones básicas de MOUT -uso de coberturas, penetración rápida en edificios, *room clearing*, tácticas de flanco, fuego de supresión, etc.- sin tener que preocuparse de controles complejos.

Sin embargo, la opción más realista y eficaz serían simuladores de alta fidelidad como *Virtual Battlespace*. Un simulador de este tipo adaptado al contexto del terrorismo seguiría la misma lógica que los ejemplos anteriores: escenarios urbanos donde el usuario ha de poner en práctica técnicas MOUT para ejecutar un atentado con éxito. Sin embargo, en lugar de tener una visión completa del mapa y un cuadro para realizar acciones con un simple click, controlaría directamente el avatar de un terrorista desde una perspectiva *first person shooter*. En este sentido, el usuario debería desplazarse y cubrirse cómo lo haría en

la realidad, pudiendo incluso ejecutar acciones concretas no disponibles en VBS, como tomar un escudo humano o estallar un cinturón bomba. En el caso de que se implantase un modo *online*, múltiples terroristas podrían conectarse para formar un grupo de fuego y llevar a cabo un atentado simulado conjuntamente. Esto generaría situaciones donde la comunicación verbal y la coordinación en combate son entrenadas. Sin duda, las mismas características que hacen de VBS una herramienta sumamente útil para el ámbito militar pueden ser trasladables a este hipotético simulador terrorista. Por ejemplo, la IA avanzada permitiría generar enemigos -en este caso policías y militares- más desafiantes, también capaces de llevar a cabo tácticas MOUT que los terroristas deberían contrarrestar. Esta IA avanzada, aplicada a los civiles -como en el motor *EXODUS* de AUGGMED- haría que no fueran simples dianas inanimadas, pues serían capaces de reaccionar de forma realista al peligro: huyendo, tratando de esconderse e incluso intentado atacar a los terroristas con armas de fortuna. Además, el *software* de la versión más reciente de VBS puede generar escenarios en base a imágenes y datos satelitales, lo cual abre la posibilidad de que los terroristas entrenen en una réplica exacta del mismo lugar que pretenden atacar en la vida real, memorizando de esta forma el terreno de antemano. Por otra parte, el simulador incluso podría incorporar elementos propios de *SanTrain* para instruir al terrorista en primeros auxilios básicos en situaciones de presión.

Por último, si el simulador anteriormente mencionado permitiera el uso de gafas VR, guantes y trajes hápticos y cintas de correr omnidireccionales, los terroristas tendrían a su disposición un método de entrenamiento completo. No solo recibirían instrucción en tácticas MOUT, sino que también mejoraría su capacidad física. Además, los actuadores térmicos y los registradores de impactos ofrecerían un *feedback* realista útil para que el usuario se acostumbre a los estímulos propios de un atentado. Respecto a la realidad aumentada, anteriormente se ha visto que esta es efectiva para mejorar la precisión en el tiro. Sin embargo, su empleo en el entrenamiento de combate urbano requiere de un escenario físico sobre el que se proyectarán las imágenes. En el contexto militar esto es una opción viable, pero no para terroristas en Occidente, los cuales llamarían demasiado la atención en el caso de “construir” un entorno de combate improvisado.

7.4. Asesinatos

Mientras que para la preparación de un asalto existen simuladores de carácter militar y policial que pueden ser readaptados a las necesidades de los terroristas, no sucede lo mismo con los asesinatos. Por razones obvias, los Estados -especialmente los democráticos- no presumirán de entrenar a individuos mediante simuladores para que sean

capaces de infiltrarse en un espacio privado y asesinar al objetivo. En consecuencia, no hay antecedentes de *serious games* cuyas mecánicas puedan siquiera ser modificadas para satisfacer esta necesidad formativa por parte del terrorismo. Sin embargo, el "mundo" de los asesinos a sueldo ha sido ampliamente tratado por videojuegos populares destinados al público general, como *Hitman*. En esta saga, el jugador encarnará a un asesino profesional con la misión de eliminar a distintos objetivos a través de múltiples escenarios 3D. El juego no es lineal, en cambio, ofrece total libertad al usuario para que pueda explorar el entorno y así escoger el mejor método de eliminación, el lugar donde cometer el asesinato o la vía de acercamiento a la víctima. En este sentido, el empleo de armas de fuego es una opción, pero por lo general el jugador sufrirá una penalización en su puntuación por haber llamado demasiado la atención. En cambio, se premia la creatividad, la reflexión y la discreción: el empleo de disfraces y tapaderas para infiltrarse en un espacio privado, encontrar métodos para que la víctima se aleje de otras personas, lograr que un paquete bomba o veneno llegue a sus manos, hacer que el asesinato parezca un accidente, etc. En la última versión se incluyó el modo *Hitman: Freelancer*, que pretende ofrecer una experiencia más realista al establecer continuidad entre escenarios -la muerte en uno de estos supone una muerte permanente que implica volver a comenzar desde cero- y un piso franco donde el jugador puede planificar asesinatos y preparar venenos o explosivos (Teuton, 2023).

Hitman no es, en absoluto, un simulador destinado al entrenamiento y a la fiel representación de la realidad. Por el contrario, es un videojuego que prioriza la diversión, por lo que simplifica muchas acciones. Sin embargo, al igual que ciertos videojuegos populares, como *Call of Duty*, inspiraron el desarrollo de simuladores militares con una perspectiva en primera persona, *Hitman* -y otros videojuegos del mismo estilo- podrían ser la base en la creación de un simulador avanzado / de alta fidelidad. Dicho simulador tomaría las mismas mecánicas expuestas anteriormente pero aumentaría su dificultad y el grado de detalle para que se aproximaran más a la realidad. Por ejemplo, que la IA tuviera un nivel elevado para que no fuera -tan- sencillo infiltrarse en un edificio privado[32] mediante un disfraz, o que elaborar un veneno -ricina o ántrax- no consistiera simplemente en reunir ciertos ingredientes y pulsar un botón, sino que implicase seguir una serie de pasos concretos basados en manuales. Incluso sería posible añadir mecánicas donde el jugador debiera eliminar u ocultar pruebas en la escena del asesinato -de forma opuesta a *Unravel the Mysterious Murder-* no para evitar la captura, pero sí para ganar tiempo. Pese a este realismo, el simulador podría conservar los elementos ludificadores -tablas de puntuación y logros- para fomentar la creatividad y las estrategias inteligentes.

[32] En este sentido, podrían emplearse sistemas de verbalización para que el usuario deba, a tiempo real, usar su voz para engañar a diferentes personajes mediante una tapadera creada por él mismo.

7.5. *“Ultimate Mowing Machine”*

El acto de arrollar a un gran grupo de peatones con un vehículo pesado es un tipo de atentado que apenas requiere de planificación y práctica. Pese a ello, ciertos grupos podrían diseñar simuladores de conducción donde el jugador ha de atropellar al máximo número de personas en un tiempo determinado. Esta idea sumamente simple podría ir acompañada de un sistema de puntuaciones y logros en función de la cantidad de víctimas provocadas. En realidad, un simulador de este tipo no tendría una finalidad formativa, sino que estaría orientado a desensibilizar al usuario y a inculcarle la asociación entre muerte y placer.

Por otra parte, los simuladores avanzados serían mucho más útiles en lo que se refiere a la modificación del vehículo. Como en *Car Mechanic Simulator*, el jugador podría interactuar con los elementos de diferentes vehículos, pero en lugar de repararlos tendría por objetivo convertirlos en armas aún más letales. Desde hace años, grupos criminales en LATAM (Longhi Bracaglia, 2011b) y el propio Estado Islámico (Al-Sudani, 2017) crean verdaderos “tanques” rudimentarios sobre la carrocería de vehículos civiles, desde camiones hasta automóviles. Mediante placas de acero soldadas y chatarra, estos vehículos obtienen una mayor resistencia frente a la munición de armas pequeñas y ligeras, lo que los convierte en instrumentos perfectos para un atentado suicida. Algunos incluso cuentan con un diseño más sofisticado e incorporan blindajes de jaula capaces de proteger el vehículo del impacto de granadas antitanque.[33] Este simulador trataría de replicar el proceso y mostraría detalladamente cómo emplear las herramientas y los componentes necesarios para añadir armas improvisadas o explosivos al vehículo, mecanismos para dispersar clavos y aceite durante una persecución (Longhi Bracaglia, 2011a) o reforzar el blindaje. Ahora bien, modificar un vehículo para dotarlo de características de este tipo requiere de amplios conocimientos mecánicos y de un taller habilitado. Por lo tanto, el simulador en cuestión no sería suficiente por sí solo para instruir a un individuo desde cero, pero podría convertirse en una fuente de inspiración y práctica para aquellos terroristas individuales o células que ya tengan experiencia previa a la hora de manipular un vehículo.

7.6. Empleo de drones como arma terrorista

Como ya se mencionó, el entrenamiento necesario para pilotar un VANT comercial es bajo ya que cuentan con sistemas que los hacen gobernables incluso para usuarios inexpertos,

[33] Inside a captured Islamic State suicide vehicle - YouTube

como navegación por satélite, piloto automático o sensores anticolisión. Sin embargo, poder pilotar el VANT no es sinónimo de saber emplearlo como arma en un atentado. En este sentido, los simuladores comerciales para instruir en el vuelo de drones podrían ser readaptados para incluir misiones donde el usuario tuviera que llevar a cabo un ataque a distancia. El hecho de que se puedan conectar controladores remotos físicos para manejar el dron virtual aumentaría el realismo y haría de estos simuladores un equivalente a los empleados por las fuerzas aéreas, pero orientado a las necesidades del terrorismo. Estas misiones podrían variar en dificultad y contemplar diferentes tipos de objetivos o métodos de ataque. Por una parte, ciertas misiones marcarían como objetivos a infraestructuras críticas, instalaciones militares, edificios públicos, personalidades importantes o simplemente aglomeraciones. A menudo tales objetivos sufren de vulnerabilidades comunes que pueden ser señaladas durante la simulación. Por otra parte, los simuladores podrían instruir en múltiples formas de emplear el dron para infringir daños, como ataques *kamikaze* con un dron bomba, ataques de dispersión aérea de explosivos, ataques de enjambre -con múltiples pilotos- o ataques indirectos -donde el dron es empleado como complemento de un ataque principal-.

Por supuesto, estos simuladores avanzados estarían acompañados de otros que previamente enseñen al usuario a modificar un dron comercial para convertirlo en un arma. Nuevamente, tomando a *DIY Simulator* o *The Workshop Game* como referencia, el usuario podría seleccionar la modificación en cuestión -y el modelo de dron empleado- para ensamblar los materiales paso a paso con su ratón. Como resultado, obtendría un dron equipado con armamento improvisado -cuchillos, dardos, bolas de hierro-, explosivos, armas de fuego, armas incendiarias, sistemas de fumigación o de dispersión de líquidos, etc. El objetivo de este tipo de simulador sería permitir al usuario ensayar antes de manipular el dron real para evitar averiarlo.

7.7. Ciberterrorismo

Aquellos individuos o grupos interesados en llevar a cabo actos de ciberterrorismo -ya sea con la finalidad de financiarse, obtener información ilícitamente o causar estragos- pueden recurrir a los *serious games* que instruyen en las bases del *hacking* ético o *penetration testing*. *X-Hacker* o *Red vs Blue: Cyber-Security Simulator* permiten al jugador actuar como un *red team*, el cuál aplica estrategias utilizadas por ciberdelincuentes reales. Sin embargo, estos consisten en *serious games* básicos o simuladores de baja fidelidad que se limitan a ofrecer nociones generales, útiles como método de introducción, pero insuficientes para aprender a superar las medidas de seguridad de un sistema o red. Al tratarse de productos

disponibles para el público general no pueden mostrar detalladamente cómo ejecutar un ciberataque, por lo que simplifican el proceso a unos pocos clicks. Por esta razón, terrorismo y delincuencia podrían colaborar para desarrollar un simulador de alta fidelidad perfeccionado gracias a los conocimientos aportados por expertos en informática de la *darknet*. Estos simuladores estarían compuestos por múltiples niveles, cada uno con una red de complejidad variable y múltiples objetivos a cumplir, desde la destrucción del sistema hasta el robo de datos sin que la víctima lo advierta. En lugar de simplificar el proceso de *hacking*, el simulador mostraría cada paso necesario ofreciendo las instrucciones adecuadas. En esencia, sería una transformación de los "cursillos" de pago que circulan por la red profunda en una plataforma interactiva para aprender *hacking* ilegal, similar a un *cyber-range*.

7.8. Estrategias para evitar la detección

Dado que las estrategias para evitar la detección dependen totalmente del contexto, los manuales no son detallistas y se centran en ofrecer consejos generales que puedan adaptarse a cualquier situación. Precisamente por esto, las instrucciones que contienen resultan, en cierta medida, ambiguas, por lo que el lector sin experiencia sufrirá un déficit de formación. Por ejemplo, los manuales insisten en la necesidad de crear un perfil falso compatible con la zona donde ha de operar el terrorista, pero apenas explican cómo hacerlo. En este sentido, los videojuegos pueden materializar y concretar tales consejos para mostrar su aplicación en diferentes escenarios simulados a modo de casos prácticos. De esta manera, el aprendiz podría identificar situaciones próximas a las que debe afrontar en su día a día y así proceder adecuadamente.

Por una parte, esta lógica podría ser reflejada en un *serious game* básico, similar a *CyberCentric, AEsOP* o *Elect BILAT*, es decir, un juego que presente su contenido en forma de narrativas y escenas donde el usuario debiera escoger con su ratón entre distintas vías de actuación para progresar. El hipotético videojuego incluiría una mecánica por turnos, donde cada turno representaría un día transcurrido. Al día, el jugador debería realizar distintas tareas para preparar un atentado: comprar materiales necesarios para un explosivo, reunirse con otro miembro de la misma célula o un traficante de armas, contactar con un posible recluta, etc. Para llevarlas a cabo, se presentarían una serie de opciones predeterminadas con diferentes consecuencias sobre dos medidores: uno relacionado con el nivel de desarrollo del atentado y el otro con el nivel de alerta por parte de las fuerzas y cuerpos de seguridad. El fin del juego se daría cuando el usuario lograra completar el desarrollo del atentado o cuando el nivel de alerta alcanzara su límite máximo, lo que

supondría el fracaso y la captura del terrorista. En función de las decisiones tomadas, ambos medidores podrían crecer o decrecer, simultáneamente o de forma inversa. El éxito, por lo tanto, dependería del equilibrio entre los dos medidores, lo que ayudaría a entender al usuario que, para planificar un atentado, en ocasiones es necesario tomar riesgos y despertar sospechas, mientras que en otras se debe sacrificar parte del progreso en la planificación para evitar ser detectado. Como consecuencia, se fomentaría el pensamiento estratégico orientado a la toma de decisiones críticas por parte del terrorista. Al margen de esta mecánica, para añadir imprevisibilidad el juego obligaría al usuario a enfrentarse a eventos que, en el caso de gestionarse incorrectamente, harían crecer notablemente el medidor de alerta: diálogos con vecinos, discusiones con el casero por recibir visitas a altas horas de la noche o, directamente, casos donde el jugador esté siendo observado por agentes de policía. Tales situaciones serían oportunidades para poner en práctica la *taqiyya*, una tapadera o tácticas de contrainteligencia. De hecho, sería posible que el sistema elaborara aleatoriamente distintos perfiles -con nombres, ocupaciones y trasfondos falsos- cuyos datos condicionaran las opciones disponibles durante el transcurso del juego. Esto forzaría al usuario a interiorizar las características del perfil si desea no ser descubierto en estos eventos.

Por otra parte, las mecánicas anteriores podrían ser perfeccionadas mediante un simulador de alta fidelidad donde la capacidad de interacción alcanzara un grado más elevado y complejo. Lo que resultaría aún más preocupante sería que este simulador fuera un MMO, es decir, un mundo virtual activo permanentemente y que permitiera la conexión de una gran cantidad de individuos. Las bases seguirían siendo las mismas: los usuarios tendrían que planificar atentados al mismo tiempo que coexisten con sus enemigos y evitan la detección por parte de los servicios de inteligencia, controlados por la IA. Pero en lugar de limitar las acciones a narrativas y escenas prediseñadas, el usuario tendría total libertad para seleccionar sus objetivos, tipologías de atentado,[34] su tapadera… Tal y como si se tratara de un *role playing game* donde el jugador puede personalizar su aventura, pero en este caso, el jugador encarnaría a un terrorista en una ciudad “hostil” llena de objetivos. Incluso podría decidir si prefiere permanecer como un terrorista individual o formar parte de una pequeña célula, lo que daría más relevancia al factor multijugador. De hecho, esto sería útil para que los terroristas aprendieran a colaborar sin despertar sospechas, determinar sistemas de comunicación propios u organizar reuniones confidenciales. Que el simulador tuviera características de MMO haría que la evolución del mundo virtual no dependiera de un único usuario. Las acciones de unos pocos generarían consecuencias a corto o largo

[34] En este sentido, el simulador podría complementarse con otros vistos anteriormente, como el destinado a fabricar explosivos o preparar asaltos.

plazo y con efectos positivos o negativos para el resto. Esto plantearía situaciones imprevisibles y obligaría a practicar la adaptabilidad frente a los desafíos. Por ejemplo, el atentado fallido de un terrorista individual provocaría un aumento de la seguridad en la zona, lo que forzaría a otra célula a modificar los planes de un futuro atentado y a prestar mayor atención a las medidas de contrainteligencia.

7.9. Obtención de información y espionaje

Existen distintas fuentes para obtener información sobre los objetivos escogidos, ya sean individuos o espacios físicos. La inteligencia de fuentes abiertas (OSINT) aporta un gran volumen de datos, pero al consistir únicamente en el análisis de redes sociales, revistas, libros o noticias emitidas por televisión no requiere ningún tipo de entrenamiento y, por lo tanto, de ningún *serious game* que la aborde. No sucede lo mismo con las fuentes ilegales. Estas permiten recolectar información sensible de carácter privado o confidencial sin que sus "propietarios" adviertan de ello. Tal operación tiene un mayor riesgo asociado, por lo que un entrenamiento previo es necesario para evitar que el terrorista sea descubierto. Sin embargo, al igual que con las estrategias para evitar la detección, en materia de espionaje los manuales se limitan a ofrecer consejos generales. En este sentido, los *serious games* serían la mejor vía -y quizá la única- a disposición del terrorismo para desarrollar habilidades de obtención de información y espionaje de forma práctica, dada la imposibilidad de recrear ejercicios de este tipo en la vida real.

Por una parte, el seguimiento y vigilancia de un individuo o la observación de lugares y edificios podrían incluirse directamente en los *serious games* sobre estrategias para evitar la detección, puesto que son temáticas estrechamente vinculadas. En el caso del *serious game* básico, algunas de las tareas necesarias para preparar un atentado podrían consistir en seguir a un funcionario del gobierno hasta su domicilio, estudiar las rutas que toma en su vehículo, observar su puesto de trabajo o tomar fotografías de la infraestructura objetivo. El jugador debería escoger entre múltiples opciones sobre cómo proceder: algunas serían las más adecuadas -dado que aplicarían los consejos generales de los manuales- y aumentarían el medidor de progreso del atentado, mientras que otras alertarían al individuo investigado o a las autoridades. Respecto al simulador avanzado, este ofrecería mucha más libertad al usuario y le permitiría seleccionar a individuos relevantes, decidir vigilar sus movimientos a pie o en vehículo, tomar fotografías del espacio en cuestión y estudiarlas posteriormente en su piso franco, etc. Por otra parte, la sustracción de documentos digitales y la interceptación de comunicaciones serían abarcadas específicamente por los simuladores avanzados de ciberterrorismo. Por último, las instrucciones referidas a la

inteligencia de fuentes humanas (HUMINT) merecerían un *serious game* propio, en concreto un simulador de baja fidelidad destinado a mejorar las habilidades de interrogación, similar a ISPO. En el ámbito policial, los ejercicios de interrogación recurren a actores que desempeñan el papel de sospechosos. El problema es que este sistema es costoso, difícil de llevar a cabo múltiples veces y el hecho de que siempre sean los mismos actores disminuye la calidad del ejercicio. En el caso del terrorismo, organizar este tipo de ejercicios es especialmente complejo para las células pequeñas e imposible para un actor solitario. Por esta razón, un *serious game* simplificaría el proceso. El objetivo sería sonsacar toda la información posible a un individuo secuestrado previamente y así conseguir datos relevantes para un futuro atentado. El jugador tendría que escoger entre distintas opciones de diálogo, algunas más efectivas que otras, y estudiar los comportamientos del secuestrado para determinar si está intentando engañarle. La dificultad variaría en función del interrogado, siendo más fácil intimidar a un encargado de la limpieza que trabaja en el edificio que se pretende atacar que a un guardaespaldas, que requerirá más tiempo y técnicas más "persuasivas". Aunque la base sería la misma que en ISPO, es evidente que no se emplearían técnicas de interrogación legales y éticas, sino que las opciones a escoger irían desde las amenazas hasta diversos métodos de tortura.

7.10. *Counter Interrogation Tactics*

Al igual que las habilidades para la interrogación, las tácticas anti interrogatorio no pueden ser adquiridas mediante la teoría, sino que requieren de práctica y una efectiva comunicación entre el aprendiz y un individuo que desempeñe el rol de interrogador policial. Pero nuevamente pueden darse los mismos obstáculos: poca o nula disponibilidad de actores y falta de experiencia a la hora de interpretar comportamientos realistas. Por esta razón, la formación en tácticas anti interrogatorio puede verse beneficiada con un *serious game* básico similar -pero con una lógica inversa- a ISPO, donde el jugador ha de evitar a toda costa revelar información al interrogador, en lugar de obtenerla. Este hipotético videojuego, como simulador de baja fidelidad, se centraría simplemente en dar a conocer al usuario qué tácticas puede emplear más allá de permanecer en silencio. Pero en vez de hacerlo mediante un manual, recurriría a la ludificación y a la puesta en práctica para que su utilización posterior resulte más intuitiva. El usuario, como terrorista individual o miembro de una célula, debería escoger entre una serie de opciones predeterminadas para tratar de no sucumbir ante la presión de los interrogadores. Tales opciones reflejarían los 9 tipos de técnicas anti interrogatorio comunes en yihadistas e individuos de extrema derecha: cambiar el tema discutido con uno no relacionado, aportar información ya conocida, retractar una afirmación -o negar que hubiera sido realizada en un primer momento-, negarse a hacer

comentarios, evitar mirar a los interrogadores, permanecer en silencio absoluto, ofrecer una respuesta improvisada, dar respuestas monosilábicas y declarar una falta de memoria. El éxito dependería de aplicar las técnicas más idóneas en función del momento y de la rapidez en la respuesta, por lo que un temporizador presionaría al usuario. Incluso podría emplearse un sistema de verbalización y una IA avanzada implantada en los interrogadores para perfeccionar las mecánicas: en lugar de seleccionar con el ratón las técnicas anti interrogatorio, el usuario debería ponerlas en práctica con su propia voz, cuyo tono o volumen sería analizado por la IA para generar diferentes respuestas.

Por otra parte, la realidad virtual podría convertirse en una herramienta de preparación emocional ante el estrés propio de los interrogatorios y de las presuntas torturas a las cuales son sometidos los sospechosos de terrorismo según su ideario extremista. La inmersividad ofrecida por las gafas de realidad virtual haría que el usuario pudiera sumergirse plenamente en una escena donde los interrogadores gritan, insultan, invaden su espacio personal y, en general, intentan quebrar su voluntad. Este simulador podría complementarse con trajes y guantes hápticos para reflejar de forma limitada -por ejemplo, mediante pequeñas descargas eléctricas, la activación de los actuadores térmicos o de los registradores de impactos- el daño sufrido por actos de tortura. Lejos de tener como finalidad mejorar la respuesta cognitiva del usuario, el simulador tendría por objetivo generar sensaciones -negativas- lo más próximas posibles a lo que supuestamente debería de afrontar el detenido para que así no sucumba rápidamente.

8. Conclusiones

En el apartado introductorio de esta investigación se explicó que, actualmente, la relación entre terrorismo y videojuegos es limitada. Por la red circulan videojuegos de contenido radical empleados exclusivamente como una forma más de difundir -con éxito- la narrativa extremista violenta en cuestión. Por el contrario, hasta la fecha no se han observado videojuegos formativos o *serious games* destinados a mejorar las habilidades y conocimientos de los terroristas, tal y como ha sucedido en el ámbito militar o policial. Sin embargo, Lakomy (2019) advierte de que esto es susceptible de cambiar, considerando que en un futuro podría darse una peligrosa combinación entre videojuegos y *open source jihad*, es decir, el contenido formativo *online* disponible para todo aquel dispuesto a ejecutar un atentado.

Es esta idea la que ha inspirado la elaboración del presente trabajo. A lo largo de todo el segundo bloque, se han estudiado las hipotéticas manifestaciones que esta combinación podría adoptar en el futuro mediante la comprensión, por una parte, de las necesidades formativas del terrorismo, y por la otra, de la industria de los *serious games*. De esta manera, se ha pretendido contestar a la pregunta de investigación original… ¿De qué formas podrían ser aprovechados los *serious games* y otras tecnologías del entretenimiento para satisfacer las necesidades formativas de los terroristas? Se ha podido comprobar que, en función de la temática y el grado de realismo perseguido, hay una gran variedad de respuestas. Desde sencillos juegos que recuerdan a un test multiopción con elementos ludificadores hasta simuladores avanzados para aprender a fabricar explosivos o donde el usuario ha de emplear todas sus capacidades físicas para ejecutar un atentado.

El potencial ofrecido -y la amenaza generada- por los *serious games* de contenido terrorista es enorme, especialmente para los terroristas individuales en Occidente, cuya fortaleza es el aislamiento, pero que cuentan con muy poca experiencia. Para los actores solitarios, llevar a cabo ejercicios reales para entrenar cualquiera de las necesidades formativas estudiadas implica romper el aislamiento y activar las alarmas de los servicios de inteligencia, por lo que acostumbran a instruirse mediante manuales y vídeos en Internet. Pero estos métodos de aprendizaje pasivo no eliminan el *amateurismo* de la mayoría de terroristas individuales, entre otras cosas, por la dificultad de poner en práctica las instrucciones y porque el contenido formativo muchas veces es elaborado por otros individuos inexpertos. Los *serious games* no están sujetos a los mismos problemas: fomentan un tipo de aprendizaje activo donde los conocimientos, sean teóricos o prácticos, son aplicados al mismo tiempo que se reciben las instrucciones, las cuales quedan

perfectamente integradas en el *gameplay*. Al transcurrir en un entorno virtual, el terrorista no requeriría colaborar con otros individuos, construir escenarios ficticios o comprar materiales, por lo que permanecería oculto. Además, los *serious games* establecen un filtro tecnológico frente al contenido formativo de baja calidad: es menos probable que un individuo inexperto se atreva a desarrollar un *serious game* puesto que es más costoso que redactar un documento. Como consecuencia de todo lo anterior, un aumento de los *serious games* podría animar a más individuos radicalizados a dar el salto final y atentar siguiendo los principios de la resistencia sin líderes. Precisamente por el riesgo de mejorar las capacidades operativas del terrorismo, los actores encargados de la seguridad no deben trivializar las características de los *serious games*, sino que han de prepararse ante una posible proliferación de este tipo de material. Tan solo bastaría que los actores principales de cada movimiento extremista comenzaran a interesarse por este medio para que dejara de formar parte de un futuro hipotético y pasara a convertirse en una innovación táctica.

Ahora bien, los *serious games* no son métodos de entrenamiento perfectos. Generalmente, son empleados como complementos de los ejercicios tradicionales, por lo que el grueso del entrenamiento no es llevado a cabo mediante estas tecnologías. Facilitan la transición entre el aprendizaje teórico y el aprendizaje *on-the-job* o práctico, pero no son sustitutivos de los medios clásicos. Lo mismo sucede en el contexto del terrorismo. A excepción del uso de drones como arma terrorista, el ciberterrorismo, las estrategias para evitar la detección, el espionaje, la interrogación y las *counter interrogation tactics*,[35] el resto de necesidades formativas pretende desarrollar capacidades físicas o habilidades manuales / técnicas. Aquí la efectividad de los *serious games* no es absoluta y muestra deficiencias. Aunque instrumentos tales cómo los guantes de realidad virtual, los trajes hápticos y las cintas omnidireccionales pretenden superar estos obstáculos, a día de hoy no ofrecen un grado de realismo suficiente como para deshacerse del entrenamiento real, solo para reducirlo.[36] El problema para los terroristas en Occidente es que, como se ha mencionado anteriormente, complementar el entrenamiento mediante *serious* games con ejercicios reales es prácticamente imposible. Por lo tanto, la dependencia frente a los *serious games* sería alta.

[35] Se trata de necesidades formativas de carácter comunicativo o sin una materialización física propiamente dicha -en el caso de las estrategias para evitar la detección, el espionaje y el ciberterrorismo- por lo que su desarrollo puede darse exclusivamente mediante *serious games*. Sucede lo mismo con los simuladores de vuelo de drones, si permiten la conexión de controladores remotos físicos se elimina la necesidad de practicar en la vida real.

[36] La única forma en la que un *serious game* podría sustituir totalmente al entrenamiento real sería incluyendo tecnología capaz de "trasladar" la mente del usuario a un personaje virtual, de forma similar a la película de ciencia ficción *MATRIX*. Bajo este supuesto, el grado de realismo e interacción serían totales, pues el cuerpo del jugador y del personaje virtual se fusionarían en uno solo, no necesitando controladores físicos de ningún tipo. Evidentemente, esto es una situación puramente ficticia, y si en un futuro se llega a desarrollar será en uno muy lejano, fuera del marco temporal establecido para esta investigación (2023-2050).

Es cierto que su nivel formativo sería notablemente mejor que el actual, basado principalmente en manuales y vídeos, pero seguiría siendo incompleto.

Otra desventaja de los *serious games* es su coste. Mientras que redactar una revista o manual con instrucciones es relativamente sencillo, diseñar un *serious game* -especialmente un simulador de alta fidelidad- exige tiempo, una gran cantidad de recursos económicos e individuos con amplios conocimientos tecnológicos. En realidad, los grandes grupos terroristas como Estado Islámico o Al-Qaeda cuentan con capacidades enormes de financiación, lo que puede observarse en sus campañas propagandísticas. Pero como se explicó en la introducción, los *serious games* son una tecnología disruptiva que se encuentra en su fase temprana, lo que provoca rechazo en ciertas organizaciones -sobre todo de tipo yihadista- que optan por priorizar los métodos tradicionales. El conservadurismo tecnológico explica principalmente el porqué no han proliferado aún videojuegos formativos de contenido terrorista. Pero es mera cuestión de tiempo que los principales ideólogos de cada movimiento empiecen a pensar que desperdiciar el potencial ofrecido por los *serious games* es un grave error, al igual que ha sucedido con las redes sociales. Hasta ese momento, se dará la misma tendencia que con los videojuegos extremistas de carácter propagandístico: los videojuegos formativos existentes serán desarrollados por individuos o pequeños grupos, muy limitados técnicamente.

Mención aparte merecen los costes desde el punto de vista del "consumidor", en este caso, los terroristas individuales o células pequeñas interesadas en entrenar a través de *serious games*. Quizá el *serious game* sea distribuido gratuitamente[37] por el desarrollador a través de foros extremistas o la *darknet*, pero para ser aprovechado adecuadamente el usuario deberá disponer de un equipo informático que cumpla con los requisitos técnicos. Un simulador de baja fidelidad puede funcionar en prácticamente cualquier ordenador, pero los simuladores de alta fidelidad, como VBS, consumen muchos recursos. Los ordenadores de mayor potencia alcanzan precios altos que pueden no estar al alcance de todos los terroristas. Esta "brecha digital" se intensifica en la adquisición de gafas VR, guantes y trajes hápticos y cintas omnidireccionales, que aún se consideran como prototipos. Este es el principal motivo por el cual la pregunta de investigación está enfocada desde un punto de vista futuro… Hasta 2050, este tipo de tecnologías avanzará rápidamente y al mismo tiempo se devaluará, lo que aumentará su accesibilidad, incluso para actores maliciosos.

[37] También cabe la posibilidad de que ciertos *serious games*, especialmente los simuladores de alta fidelidad, adquieran un carácter confidencial e interno, como *Al Qaeda Handbook*. Únicamente serían distribuidos a individuos selectos para evitar la filtración de métodos, estrategias y tácticas empleadas por el grupo terrorista en cuestión.

Para finalizar, quisiera comentar brevemente un tema que no forma parte del objeto de estudio de la presente investigación, pero guarda un tipo de relación inversa con este… Los videojuegos para la desradicalización. En todo momento, el enfoque se ha puesto en la relación entre videojuegos o terrorismo, ya sea con finalidad propagandística o formativa. Pero no se ha analizado el cómo los videojuegos podrían ayudar a combatir el terrorismo. Con esto no me refiero a los *serious games* destinados a mejorar las habilidades de los cuerpos policiales para intervenir en un atentado, o la capacidad de detección del peligro por parte de los servicios de inteligencia. En cambio, me refiero a videojuegos que actúen a modo de contrapropaganda, destinados a derribar las bases de una narrativa extremista violenta. Hasta la fecha se han iniciado varios proyectos de este tipo, como *DECOUNT*. *DECOUNT* es un juego de navegador -un "simulador" de baja fidelidad, según los términos empleados en este trabajo- que recrea los procesos de radicalización de 4 jóvenes. Tiene por objetivo mostrar al usuario cómo se produce este fenómeno, sus consecuencias a nivel social y cómo detectarlo preventivamente (Pisoiu y Lippe, 2022). Pero se trata de ideas cuyo potencial aún está por desarrollar -e investigar- y es que, nuevamente, se trivializa la influencia de los videojuegos al ser considerados como tecnologías disruptivas. Sin embargo, tarde o temprano las agencias encargadas de evitar la radicalización violenta mediante discursos alternativos deberán considerar su utilización, principalmente porque los grupos terroristas ya lo hacen con éxito. En la sociedad actual, marcada por la gratificación inmediata y la superficialidad, la racionalidad del mensaje cede importancia ante la "estética". En este sentido, poco importa que los argumentos en contra de la radicalización sean válidos y estructurados si el mensaje ofrecido por los movimientos extremistas, pese a ser erróneo, llega a un público más extenso al recubrirse de una capa atractiva mediante videojuegos, vídeos musicales o películas de acción propagandísticas. Por esta razón, las contra narrativas han de actualizarse y adoptar una forma mucho más cercana a las generaciones jóvenes, al fin y al cabo son el objetivo del terrorimo.

Ahora bien, se ha de evitar a toda costa desarrollar videojuegos cuyo concepto de contrapropaganda sea la demonización de los movimientos extremistas. La mayoría de videojuegos comerciales que tratan temáticas relacionadas con el terrorismo -*Call of Duty, Medal of Honor: Warfighter, Splinter Cell*, etc.- glorifican las aspiraciones políticas occidentales y simplifican las narrativas extremistas, tratando a los terroristas como psicópatas motivados por el mero deseo de provocar daños sin sentido alguno (Schulzke, 2013). La realidad demuestra que esto no es así y desarrollar narrativas alternativas de este tipo puede ser contraproducente para lograr que un individuo en proceso de radicalización "escape" de las garras del extremismo, pues se está reforzando la visión dicotómica y la hostilidad. Retroalimentar el odio no es la solución, pues lo único que se consigue es un

mayor aislamiento por parte del radicalizado. En cambio, se ha de potenciar la oportunidad que ofrecen los videojuegos para ponerse en la piel de otros para así fomentar la empatía, la comprensión y acabar con los pilares de las narrativas violentas, los cuales se basan en la ignorancia y el odio.

Bibliografía

Aarsen, J. (2017). Guerrilla and Terrorist Training Manuals. Comparing classical guerrilla manuals with contemporary terrorist manuals (AQ & IS). [Tesis de Maestría, Universidad de Leiden] . https://studenttheses.universiteitleiden.nl/handle/1887/83821

Akhgar, B. (2019). Serious Games for Enhancing Law Enforcement Agencies (Springer ed.). https://link.springer.com/book/10.1007/978-3-030-29926-2

Al Qaeda militants kill American hostage. (19/06/2004). CNN.com. Fecha de consulta (17/02/2023) http://edition.cnn.com/2004/WORLD/meast/06/18/saudi.kidnap/

Al Qaeda Training Manual. (n.d.). Fecha de consulta (11/02/2023) https://irp.fas.org/world/para/manualpart1.html

al-Muqrin, A. A. (n.d.). Al Qaeda kidnapping manual. Fecha de consulta (02/11/2023) https://www.nytimes.com/interactive/2014/07/30/world/africa/31kidnap-docviewer3.html

Al-Sudani, T. (19/07/2017). Islamic State 's customised car bombs. The Guardian. Fecha de consulta: (08/04/2023). https://www.theguardian.com/world/gallery/2017/jul/19/islamic-state-customised-car-bombs-iraq-pictures

Alandete, D. (12/10/2011). Juicio al nigeriano que intentó volar un avión a Detroit en nombre de Al Qaeda. EL PAÍS. Fecha de consulta (18/02/2023). https://elpais.com/internacional/2011/10/12/actualidad/1318400652_154294.html?event_log=go

Alhadeff, E. (13/11/2019). Serious Game To Understand Hacking Workflows. SERIOUS GAME MARKET. Fecha de consulta: (26/03/2023). https://www.seriousgamemarket.com/2019/11/serious-game-to-understand-hacking.html

Alison, L., Alison, E., Noone, G., Elntib, S., Waring, S. y Christiansen, P. (2014). Whatever you say, say nothing: Individual differences in counter interrogation tactics amongst a field sample of right wing, AQ inspired and paramilitary terrorists. Personality and Individual Differences, 68, 170-175. https://doi.org/10.1016/j.paid.2014.04.031

Almaraz Sánchez, S. I. (10/10/2022). Tráfico de armas pequeñas y ligeras: el coste de subestimar la amenaza. Instituto Español de Estudios Estratégicos. https://www.ieee.es/publicaciones-new/documentos-de-opinion/2022/DIEEEO88_2022_SERALM_Armas.html

Anderer, J. (03/09/2019). Hurry Up! Modern Patience Thresholds Lower Than Ever Before, Survey Finds. Study Finds. Fecha de consulta (20/01//2023). https://studyfinds.org/hurry-up-modern-patience-thresholds-lower-than-ever-before-survey-finds/

Anderson, C., & Dill, K. (2000). Video Games and Aggressive Thoughts, Feelings, and Behavior in the Laboratory and in Life. Journal of Personality and Social Psychology, 78(4), 772-790. 10.1037//0022-3514.78.4.772

Arias Gil, E. (2018). La estrategia y táctica terrorista de los actores individuales en la extrema derecha estadounidense. Revista UNISCI, (47), 247-264. https://dialnet.unirioja.es/servlet/articulo?codigo=6826770

Assolini, F. (16/01/2012). A School for Cybercrime: How to Become a Black Hat. Securelist. Fecha de consulta (05/03/2023). https://securelist.com/a-school-for-cybercrime-how-to-become-a-black-hat/32084/

Atkinson-Bonasio, A. (29/08/2008). Video Games in Military Training: An Interview with Roger Smith. The escapist. Fecha de consulta (19/03/2023) http://www.simulationfirst.com/papers/RSmith_Escapist_080829.pdf

Aupperlee, A. (30/09/2021). Learning is more effective when active. ScienceDaily. Fecha de consulta (21/01/2023) https://www.sciencedaily.com/releases/2021/09/210930140710.htm

Backlund, P., Johannesson, M., Engstrom, H. y Lebram, M. (2007). Sidh - a Game Based Firefighter Training Simulation. 11th International Conference Information Visualization, 899-907. 10.1109/IV.2007.100

Ballesteros, R. R. (27/07/2020). Fake passports: así es el mercado negro de DNI y pasaportes falsos en Telegram. El Confidencial. Fecha de consulta (28/02/2023) https://www.elconfidencial.com/espana/2019-12-24/asi-funciona-mercado-negro-pasaportes-dni-telegram_2386232/

Bandura, A. (1990). Selective Activation and Disengagement of Moral Control. Journal of Social Issues, 46(1), 27-46. https://doi.org/10.1111/j.1540-4560.1990.tb00270.x

Berglund, N. (09/02/2012). Breivik 'addicted to computer games'. Norway's News in English. Fecha de consulta (03/02/2023) https://www.newsinenglish.no/2012/02/09/breivik-addicted-to-computer-games/

Bloom's Taxonomy. (n.d.). University of Waterloo. Fecha de consulta (19/03/2023) https://uwaterloo.ca/centre-for-teaching-excellence/catalogs/tip-sheets/blooms-taxonomy

Boston Marathon bombing trial jury sees pipe bombs tossed at police. (19/03/2015). CBS News. Fecha de consulta (18/02/2023). https://www.cbsnews.com/news/boston-marathon-bombing-trial-jury-pipe-bombs/

Breivik, A. (2011). 2083: Una Declaración Europea de Independencia. Fecha de consulta (14/02/2023) https://sites.google.com/site/breivikmanifesto/2083/book-3

Bruzzone, A., Tremori, A., & Massei, M. (01/10/2009). Serious Games for Training and Education on Defense against Terrorism. Defense Technical Information Center. Fecha de consulta (27/03/2023). https://apps.dtic.mil/sti/citations/ADA568206

Béthencourt, Á. (28/12/2017). Amateurismo yihadista. Observatorio Internacional de Estudios sobre Terrorismo. Fecha de consulta (28/01/2023) https://observatorioterrorismo.com/analisis/amateurismo-yihadista/

Baqués, J., Toboso, M., & Ortolà, C. (2022). El manifiesto terrorista como instrumento de análisis del proceso de radicalización: el caso de la extrema derecha. Revista de Estudios en Seguridad Internacional, 8(1), 143-163. https://seguridadinternacional.es/resi/html/el-manifiesto-terrorista-como-instrumento-de-analisis-del-proceso-de-radicalizacion-el-caso-de-la-extrema-derecha/

Car Mechanic Simulator: how realism is best for education. (17/11/2021). Study International. Fecha de consulta: (31/03/2023). https://www.studyinternational.com/news/car-mechanic-simulator/

CENTRIC Cyber Winning National Awards. (06/06/2019). CENTRIC. Fecha de consulta (26/03/2023). https://research.shu.ac.uk/centric/news/centric-cyber-winning-national-awards/

Coombes, L. (23/03/2021). Six Days In Fallujah Will Use Procedurally Generated Maps. Gfinity Esports. Fecha de consulta (31/03/2023) https://www.gfinityesports.com/gaming-news/six-days-in-fallujah-will-use-procedurally-generated-maps/

Crece el público gamer: un estudio revela sus ganancias y tendencias esenciales para este año. (22/05/2022). Forbes Colombia. Fecha de consulta (23/01/2023) https://forbes.co/2022/05/22/actualidad/crece-el-publico-gamer-un-estudio-revela-sus-ganancias-y-tendencias-esenciales-para-este-ano

Davidson, H. (22/09/2014). Islamic State's call to kill westerners has terrorism experts divided. The Guardian. https://www.theguardian.com/world/2014/sep/23/islamic-states-call-to-kill-westerners-has-terrorism-experts-divided

de Armas, C., Tori, R. y Valerio Netto, A. (2020). Use of virtual reality simulators for training programs in the areas of security and defense: a systematic review. Multimedia Tools and Applications, 79, 3495–3515. https://doi.org/10.1007/s11042-019-08141-8

Defensa Activa e Inteligencia: Threat Intelligence en los entornos industriales. (06/09/2018). INCIBE-CERT. Fecha de consulta (05/03/2023) https://www.incibe-cert.es/blog/defensa-activa-e-inteligencia-threat-intelligence-los-entornos-industriales

Dobrovsky, A., Borghoff, U., y Hofmann, M. (2017). Applying and Augmenting Deep Reinforcement Learning in Serious Games through Interaction. Periodica Polytechnica Electrical Engineering and Computer Science, 61(2), 198-208. https://doi.org/10.3311/PPee.10313

Dolven, T. y Fidel, E. (27/12/2017). This prison is using VR to teach inmates how to live on the outside. VICE. Fecha de consulta (02/04/2023) https://www.vice.com/en/article/bjym3w/this-prison-is-using-vr-to-teach-inmates-how-to-live-on-the-outside

Drakou, M., & Lanitis, A. (2016). On the Development and Evaluation of a Serious Game for Forensic Examination Training. 18th Mediterranean Electrotechnical Conference (MELECON), 1-6. https://ieeexplore.ieee.org/document/7495415

Drone Flight Simulators: Your Guide to the Top 8 Drone Simulators of 2022. (n.d.). UAV Coach. Fecha de consulta (31/03/2023) https://uavcoach.com/drone-flight-simulator/#guide-2

Díez Cámara, O. (26/10/2021). VIRTRA, el simulador de tiro en que se adiestrarán los Mossos d'Esquadra. Defensa.com. Fecha de consulta (01/04/2023) https://www.defensa.com/espana/virtra-simulador-tiro-adiestraran-mossos-desquadra

E-Book Distributed Via Twitter: 'How To Survive In The West – A Mujahid Guide'. (03/05/2015). MEMRI. Fecha de consulta (17/02/2023) https://www.memri.org/jttm/e-book-distributed-twitter-how-survive-west-%E2%80%93-mujahid-guide

El Ejército diseña un sistema de adiestramiento de realidad aumentada. (28/06/2019). Infodefensa. Fecha de consulta (02/04/2023). https://www.infodefensa.com/texto-diario/mostrar/3129539/ejercito-disena-sistema-adiestramiento-realidad-aumentada

El neonazi de Halle podría haber fabricado sus armas en una impresora 3D. (11/10/2019). La Vanguardia. Fecha de consulta (19/02/2023) https://www.lavanguardia.com/internacional/20191011/47901882921/neonazi-halle-fabricado-armas-impresora-3d-motivacion-antisemita.html

Esparragoza, B. (22/02/2021). Armas 'hechizas': una estrategia barata del crimen. El Heraldo. Fecha de consulta (27/02/2023) https://www.elheraldo.co/judicial/armas-hechizas-una-estrategia-barata-del-crimen-796588

EU Counter-Terrorism Coordinator. (06/07/2020). Online gaming in the context of the fight against terrorism. https://data.consilium.europa.eu/doc/document/ST-9066-2020-INIT/en/pdf

Evans, R. (04/08/2019). The El Paso Shooting and the Gamification of Terror. Bellingcat. Fecha de consulta (24/01/2023) https://www.bellingcat.com/news/americas/2019/08/04/the-el-paso-shooting-and-the-gamification-of-terror/

Federation of American Scientists. (2006). Summit on educational games: Harnessing the power of video games for learning. Fecha de consulta (19/03/2023) https://www.informalscience.org/sites/default/files/Summit_on_Educational_Games.pdf

Ferguson, C. (2011). Video Games and Youth Violence: A Prospective Analysis in Adolescents. Journal of Youth and Adolescence, 40, 377-391. 10.1007/s10964-010-9610-x

Fernández Nieto, I. (2018). La letalidad del ciberterrorismo. Revista general de Marina, 275, 133-142. https://dialnet.unirioja.es/servlet/articulo?codigo=6518327

Gault, M. (16/06/2015). Islamic State's 'How to Survive in the West' Handbook Is Really Dumb. Medium. Fecha de consulta (16/02/2023) https://medium.com/war-is-boring/islamic-state-s-how-to-survive-in-the-west-probably-wasn-t-written-by-islamic-state-9f41c41eb45

Gill, P., Horgan, J., & Deckert, P. (2013). Bombing Alone: Tracing the Motivations and Antecedent Behaviors of Lone-Actor Terrorists. Journal of Forensic Sciences, 59(2), 425-435. https://doi.org/10.1111/1556-4029.12312

González, E. (09/02/2021). Individualismo, enemigo de la ciudadanía del siglo XXI. Fundación Rafael del Pino. Fecha de consulta (28/01/2023) https://frdelpino.es/actualidad/individualismo-enemigo-de-la-ciudadania-del-siglo-xxi/

Gorman, C. (2012). GETTING SERIOUS ABOUT GAMES—USING VIDEO GAME-BASED LEARNING TO ENHANCE NUCLEAR TERRORISM PREPAREDNESS. [Tesis de maestría, Naval Postgraduate School]. Dudley Knox Library. https://calhoun.nps.edu/handle/10945/6803

Grizzard, M., Tamborini, R., Sherry, J., Weber, R., Prabhu, S., Hahn, L. y Idzik, P. (2014). The Thrill Is Gone, but You Might Not Know: Habituation and Generalization of Biophysiological and Self-reported Arousal Responses to Video Games. Communication Monographs, 82(1), 64-87. https://doi.org/10.1080/03637751.2014.971418

Grossman, D. (10/08/1998). Trained to Kill. Christianity Today. Fecha de consulta (02/02/2023) https://www.christianitytoday.com/ct/1998/august10/8t9030.html?order=&start=12

Guimarães, M., Prada, R., Santos, P., Dias, J., Soeiro, C., Guerra, R., Steiner-Stanitznig, C. y Molinari, A. (08/11/2022). ISPO: A Serious Game to train the Interview Skills of Police Officers. International Journal of Serious Games, 9(4), 43-61. https://doi.org/10.17083/ijsg.v9i4.514

HaptX abre la pre-compra de sus guantes Gloves G1. (25/10/2022). RealoVirtual. Fecha de consulta (01/04/2023) https://www.realovirtual.com/noticias/12004/haptx-abre-pre-compra-sus-guantes-gloves-g1

Haskins, S. (04/02/2020). VR Exposure Therapy Provides Treatment Option for PTSD. VR Fitness Insider. Fecha de consulta (02/04/2023). https://www.vrfitnessinsider.com/vr-exposure-therapy-provides-treatment-option-for-ptsd/

Hayden, S. (16/04/2018). Researchers Electrically Stimulate Muscles in Haptic Designed for Hands-free AR Input. Road to VR. Fecha de consulta (01/04/2023) https://www.roadtovr.com/researchers-electrically-stimulate-muscles-haptic-designed-hands-free-ar-input/

Hill, R., Belanich, J., Lane, C., Core, M., Dixon, M., Forbell, E., Kim, J., y Hart, J. (01/01/2006). Pedagogically Structured Game-Based Training: Development of the Elect BiLAT Simulation. Defense Technical Information Center. Fecha de consulta (27/03/2023) https://apps.dtic.mil/sti/citations/ADA461575

Holden, M. (26/07/2011). Los Caballeros Templarios de Europa: ¿extrema derecha o ficción? Reuters. Fecha de consulta (04/03/2023) https://www.reuters.com/article/internacional-noruega-caballeros-europa-idLTASIE76Q00A20110727

Horejší, P., Vyšata, J., Rohlíková, L., Polcar, J., & Gregor, M. (2019). Serious Games in Mechanical Engineering Education. Research & Innovation Forum 2019, 55-63. https://link.springer.com/chapter/10.1007/978-3-030-30809-4_6

How to survive in the west: A mujahid guide. (2015). Fecha de consulta (15/02/2023) https://blazingcatfur.ca/wp-content/uploads/2015/04/ISIS-How-to-survive-in-the-west.pdf

Hsu, J. (16/09/2011). Terrorists Use Online Games to Recruit Future Jihadis. NBC News. Fecha de consulta (24/01/2023) https://www.nbcnews.com/id/wbna44551906#.Xf-ydUdKg2w

Irish Republican Army. (n.d.). IRISH REPUBLICAN ARMY “GREEN BOOK” (Volumes I & II). Internet Archive. Fecha de consulta (10/02/2023) https://archive.org/details/ira-green-book-volumes-1-and-2/mode/2up

Jiménez, P. (14/09/2017). El youtuber de Marmolejo absuelto por fabricar armas y condenado por tenerlas. Cadena SER. Fecha de consulta (27/02/2023) https://cadenaser.com/emisora/2017/09/14/ser_andujar/1505390591_474284.html

La policía eleva a 92 los muertos por el doble atentado en Noruega. (23/07/2011). EL PAÍS. Fecha de consulta (28/01/2023) https://elpais.com/internacional/2011/07/23/actualidad/1311372004_850215.html?event=go&event_log=go&prod=REGCRART&o=cerrado

Lakomy, M. (2019). Let's Play a Video Game: Jihadi Propaganda in the World of Electronic Entertainment. Studies in Conflict & Terrorism, 42(4), 383-406. https://doi.org/10.1080/1057610X.2017.1385903

Longhi Bracaglia, I. (08/06/2011b). Un taller casero para 'monstruos', los camiones blindados de los 'narcos' | México. El Mundo. Fecha de consulta: (08/04/2023) https://www.elmundo.es/america/2011/06/06/mexico/1307395547.html

Longhi Bracaglia, I. (12/05/2011a). El nuevo 'coche fantástico' de los Zetas. El Mundo. Fecha de consulta: (08/04/2023) https://www.elmundo.es/america/2011/05/10/mexico/1305053816.html

Lopez Fonseca, Ó. (14/06/2022). Un menor se cuela en el centro policial más seguro y vigilado de España y roba dos pistolas. El País. Fecha de consulta (19/02/2023) https://elpais.com/espana/2022-06-14/roban-dos-pistolas-en-el-centro-policial-mas-seguro-de-espana.html?event_log=go

Los autores del tiroteo de California dejaron a su bebé a la abuela. (10/10/2017). El Periódico. Fecha de consulta (25/02/2023) https://www.elperiodico.com/es/internacional/20151203/tiroteo-california-perfil-autores-masacre-san-bernardino-4722615

Los terroristas iban a atentar en el centro comercial Puerta de Europa. (07/08/2012). Europa Sur. Fecha de consulta (24/02/2023) https://www.europasur.es/algeciras/terroristas-atentar-comercial-Puerta-Europa_0_613439062.html

Marighella, C. (1969). MINIMANUAL DEL GUERRILLERO URBANO. https://dialnet.unirioja.es/servlet/articulo?codigo=4771592

Markey, P., Ivory, J., Slotter, E., Oliver, M. B. y Maglalang, O. (2020). He Does Not Look Like Video Games Made Him Do It: Racial Stereotypes and School Shootings. Psychology of Popular Media Culture, 9(4), 493-498. https://doi.org/10.1037/ppm0000255

Markey, P., Markey, C., & French, J. (2015). Violent Video Games and Real-World Violence: Rhetoric Versus Data. Psychology of Popular Media Culture, 4(4), 277-295. https://doi.org/10.1037/ppm0000030

Martínez González, M., Robles Haydar, C. y Alfaro Alvarez, J. (2020). Concepto de desconexión moral y sus manifestaciones contemporáneas. Utopía Y Praxis Latinoamericana, 25(11), 349-361. https://produccioncientificaluz.org/index.php/utopia/article/view/34525

Marín Delgado, J. A. (29/01/2018). El uso de drones comerciales como vectores terroristas. Instituto Español de Estudios Estratégicos. https://dialnet.unirioja.es/servlet/articulo?codigo=6467970

Moghaddam, F. (2005). The Staircase to Terrorism: A Psychological Exploration. American Psychologist, 60(2), 161-169. https://doi.org/10.1037/0003-066X.60.2.161

Moroccan Sentenced to 2 Years for 'Plotting' to Attack Harvard University. (30/10/2014). Morocco World News. Fecha de consulta (24/02/2023) https://www.moroccoworldnews.com/2014/10/142749/moroccan-sentenced-to-2-years-for-plotting-to-attack-harvard-university-2

Moyano Pacheco, M. (2020). La radicalización violenta. Unidad didáctica para Psicología. 2º Bachillerato. Dirección General de Apoyo a Víctimas del Terrorismo. Ministerio del Interior. https://sede.educacion.gob.es/publiventa/la-radicalizacion-violenta-unidad-didactica-para-psicologia-2-bachillerato/bachillerato-historia-terrorismo/23998

New Federal De-Escalation Grant Program Will Improve Opportunities for Mental Health Intervention for State & Local Agencies. (08/03/2023). Axon. Fecha de consulta (02/04/2023) https://www.axon.com/news/federal-de-escalation-grant

Nichols, P. (17/07/2019). Tactical Decision-making Simulations. Marine Corps Association. Fecha de consulta (27/03/2023) https://mca-marines.org/blog/gazette/tactical-decision-making-simulations/

Nine out of ten employees need basic cybersecurity skills training. (25/10/2022). Kaspersky. Fecha de consulta (05/03/2023) https://www.kaspersky.com/about/press-releases/2022_nine-out-of-ten-employees-need-basic-cybersecurity-skills-training

Observatorio Internacional de Estudios sobre Terrorismo [OIET]. (2021). Anuario del terrorismo yihadista 2021. https://observatorioterrorismo.com/anuarios-del-terrorismo-yihadista/

Orvis, K., Moore, J., Belanich, J., Murphy, J. y Horn, D. (2010). Are Soldiers Gamers? Videogame Usage among Soldiers and Implications for the Effective Use of Serious Videogames for Military Training. MILITARY PSYCHOLOGY, 22, 143-157. https://doi.org/10.1080/08995600903417225

Papakonstantinou, V. (2022). The Cybersecurity Obligations of States Perceived as Platforms: Are Current European National Cybersecurity Strategies enough? Applied Cybersecurity & Internet Governance, 1(1), 1-12. https://doi.org/10.5604/01.3001.0016.1237

Paris terror arsenal: Kalashnikovs, rocket launcher and grenades. (11/01/2015). The Malta Independent. Fecha de consulta (19/02/2023) https://www.independent.com.mt/articles/2015-01-11/world-news/Paris-terror-arsenal-Kalashnikovs-rocket-launcher-and-grenades-6736128492

Peck, M. (02/01/2005). Soldiers Learn Hazards Of War in Virtual Reality. National Defense Magazine. Fecha de consulta (31/03/2023) https://www.nationaldefensemagazine.org/articles/2005/1/31/2005february--soldiers-learn-hazards-of-war-in-virtual-reality

Peña Alonso, J. A. (2019). LA EVOLUCIÓN DEL TERRORISMO EN LA PRÓXIMA DÉCADA. [Trabajo Final de Grado, Universidad de Barcelona] https://www.recercat.cat/bitstream/handle/2072/359727/Pe%c3%b1a%20Alonso%2c%20Jos%c3%a9%20Antonio.pdf?sequence=1

Peñalosa, G. (26/01/2023). Yasin Kanza, el yihadista de Algeciras, increpaba en la calle a las mujeres y exaltaba en redes sociales a Daesh. El Mundo. Fecha de consulta (27/01/2023) https://www.elmundo.es/espana/2023/01/26/63d2cf1c21efa0886a8b45a3.html

Pidd, H. (19/04/2012). Anders Breivik 'trained' for shooting attacks by playing Call of Duty. The Guardian. https://www.theguardian.com/world/2012/apr/19/anders-breivik-call-of-duty

Pieslak, J. (2017). "A Musicological Perspective on Jihadi anashid" in Jihadi Culture: The Art and Social Practices of Militant Islamists (Cambridge University Press ed.). Thomas Hegghammer. https://doi.org/10.1017/9781139086141

Pisoiu, D., & Lippe, F. (2022). The name of the game: Promoting resilience against extremism through an online gaming campaign. FIRST MONDAY, 27(5). https://doi.org/10.5210/fm.v27i5.12600

RAN Health and Social Care. (2017). Risk assessment of lone actors. https://home-affairs.ec.europa.eu/system/files_en?file=2020-09/ran_h-sc_risk_assessment_lone_actors_11-12_12_2017_en.pdf

Robson, K., Plangger, K., Kietzmann, J., McCarthy, I. y Pitt, L. (2016). Game on: Engaging customers and employees through gamification. Business Horizons, 59(1), 29-36. https://doi.org/10.1016/j.bushor.2015.08.002

Robson, S. (23/01/2006). DARWARS: Helping the force fight insurgents. Stars and Stripes. Fecha de consulta (31/03/2023) https://www.stripes.com/news/darwars-helping-the-force-fight-insurgents-1.43894

Rueda, S., Ferguson, C., Cruz, A., Ferguson, D., Fritz, S. y Smith, S. (2008). Violent Video Games and Aggression: Causal Relationship or Byproduct of Family Violence and Intrinsic Violence Motivation? Criminal Justice and Behavior, 35(3), 311-332. https://doi.org/10.1177/0093854807311719

Rus, C. (07/10/2020). Virtuix Omni One, 2000 dólares por una cinta de correr en 360 grados para realidad virtual. Xataka. Fecha de consulta (01/04/2023) https://www.xataka.com/otros-dispositivos/virtuix-omni-one-cinta-correr-360-grados-pensada-para-moverse-entornos-realidad-virtual

Samčović, A. (2018). SERIOUS GAMES IN MILITARY APPLICATIONS. Vojnotehnički glasnik, 66(3), 597-613. https://doi.org/10.5937/vojtehg66-16367

San Ruperto, M. G. (2005). Grupos Radicales Islámicos en la Red. Revista Historia y Comunicación Social, 10, 117-133. https://revistas.ucm.es/index.php/HICS/article/view/HICS0505110117A

Sandberg, S., Jensen, S. Q., & Larsen, J. F. (2021). Rap, Islam and Jihadi Cool: The attractions of the Western jihadi subculture. Crime, Media, Culture: An International Journal, 18(3), 1-16. https://doi.org/10.1177/17416590211025573

Schlegel, L. (13/04/2020b). How Video Games Could Facilitate Radicalization Processes. Security Web Portal. Fecha de consulta (20/01/2023) https://www.rcc.int/swp/news/278/how-video-games-could-facilitate-radicalization-processes

Schlegel, L. (2020a). Jumanji Extremism? How games and gamification could facilitate radicalization processes. Journal for deradicalization, Summer 2020(23), 1-44. https://journals.sfu.ca/jd/index.php/jd/article/view/359

Schrijvers, E., Prins, C. y Passchier, R. (2021). Preparing for Digital Disruption. Springer. https://doi.org/10.1007/978-3-030-77838-5

Schulzke, M. (2013). Being a terrorist: Video game simulations of the other side of the War on Terror. Media, War & Conflict, 6(3), 207-220. https://doi.org/10.1177/1750635213494129

Selepak, A. (2010). Skinhead Super Mario Brothers: An Examination of Racist and Violent Games on White Supremacist Web Sites. Journal of Criminal Justice and Popular Culture, 17(1), 1-47.

Simpson, J. (15/01/2014). ‘Door Kickers’ Breathes Life Into Tactical Games. War Is Boring. Fecha de consulta (30/03/2023) https://warisboring.com/door-kickers-breathes-life-into-tactical-games/

Smith, P. (06/11/2013). Serious Games 101. Serious Games and Their Use in NATO, 1-12. https://www.sto.nato.int/publications/STO%20Educational%20Notes/Forms/Educational%20Notes%20Document%20Set/docsethomepage.aspx?ID=3482&FolderCTID=0x012000D52000078F9E87043356C409A0D30823AFA16F60300099FA443AE6E08499A57A0FBE0134F20&List=44a8f49d-e481-458a-91b4-

Sormani, R., Soldatos, J., Vassilaras, S., Kioumourtzis, G., Leventakis, G., Giordani, I. y Tisato, F. (2016). A serious game empowering the prediction of potential terrorist actions. Journal of Policing, Intelligence and Counter Terrorism, 11(1), 30-48. https://doi.org/10.1080/18335330.2016.1161222

Stenersen, A. (2008). The Internet: A Virtual Training Camp? Terrorism and Political Violence, 20(2), 215-233. https://doi.org/10.1080/09546550801920790

Sánchez Morales, R. (2020). MEJORA DE LA INSTRUCCIÓN Y EL ADIESTRAMIENTO DE UN ESCUADRÓN LIGERO ACORAZADO EN ENTORNO VIRTUAL. [Trabajo Final de Grado, Universidad de Zaragoza]. https://zaguan.unizar.es/record/101020?ln=es#

Teuton, C. (07/02/2023). Hitman: Freelancer Review - Agent 47 At His Best. Screen Rant. Fecha de consulta: (09/04/2023). https://screenrant.com/hitman-freelancer-pc-review/

Thiagarajan, S. (1998). The Myths and Realities of Simulations in Performance Technology. Educational Technology, 38(5), 35-41. http://www.jstor.org/stable/44428481

Thurrott, P. (16/11/2001). Microsoft Flight Simulator in Terrorist Controversy. ITPro Today. https://www.itprotoday.com/windows-78/microsoft-flight-simulator-terrorist-controversy

Toboso Buezo, M. (2019). TERRORISME I ANTITERRORISME. Institut de Seguretat Pública de Catalunya. 978-84-393-9950-6

Toboso, M. (13/01/2016). El terrorismo individual durante el año 2015: Recalibrando la amenaza. Grupo de Estudios en Seguridad Internacional [GESI]. http://www.seguridadinternacional.es/?q=es/content/el-terrorismo-individual-durante-el-a%C3%B1o-2015-recalibrando-la-amenaza

Toboso, M. (2015, 02 10). El terrorismo individual durante el año 2014: ¿Un fenómeno marginal o una tendencia al alza? | GESI. Grupo de Estudios en Seguridad Internacional (GESI). Fecha de consulta (27/01/2023) https://www.seguridadinternacional.es/?q=es/content/el-terrorismo-individual-durante-el-a%C3%B1o-2014-%C2%BFun-fen%C3%B3meno-marginal-o-una-tendencia-al-alza

Toboso, M. (08/02/2022). Terrorismo individual: la derivada de la sociedad actual. Global Strategy. Fecha de consulta (28/01/2023) https://global-strategy.org/terrorismo-individual-la-derivada-de-la-sociedad-actual/

Una banda de narcos de la marihuana activa un parany per disparar contra Mossos al Segrià. (08/09/2021) XCatalunya.cat. Fecha de consulta (27/02/2023) https://www.xcatalunya.cat/narcos-marihuana-atac-segria/

UNITED STATES SECRET SERVICE AND UNITED STATES DEPARTMENT OF EDUCATION. (2004). THE FINAL REPORT AND FINDINGS OF THE SAFE SCHOOL INITIATIVE: IMPLICATIONS FOR THE PREVENTION OF SCHOOL ATTACKS IN THE UNITED STATES. Fecha de consulta (03/02/2023) https://www2.ed.gov/admins/lead/safety/preventingattacksreport.pdf

Val, E. (10/10/2019). El vídeo del ataque del neonazi que mató a dos personas en una sinagoga. La Vanguardia. Fecha de consulta (25/01/2023) https://www.lavanguardia.com/internacional/20191010/47888238735/neonazi-stephan-balliet-ataque-sinagoga-halle-alemania-streaming-twitch.html

van Roy, R., & Zaman, B. (2019). Unravelling the ambivalent motivational power of gamification: A basic psychological needs perspective. International Journal of Human-Computer Studies, 127, 38-50. https://doi.org/10.1016/j.ijhcs.2018.04.009

Veloso, N. (16/03/2019). Por 'streaming' y a una audiencia planetaria: Nueva Zelanda sufre el primer gran atentado viral. El Español. Fecha de consulta (25/01/2023) https://www.elespanol.com/mundo/20190316/streaming-audiencia-planetaria-nueva-zelanda-primer-atentado/383462906_0.html

Vonow, B. (17/03/2019). NZ shooter's gran reveals how he went from nerd scared of girls to terrorist. The Sun. Fecha de consulta (03/02/2023) https://www.thesun.co.uk/news/8655284/new-zealand-mosque-shooter-brenton-tarrant-gran/

Wall, D. (18/11/2014). 'High risk' cyber-crime is really a mixed bag of threats. Durham University. Fecha de consulta (05/03/2023) https://www.dur.ac.uk/news/allnews/thoughtleadership/?itemno=22869

Wei, L., Zhou, H., & Nahavandi, S. (2019). Haptically enabled simulation system for firearm shooting training. Virtual Reality, Augmented Reality and Commerce, 23, 217-228. https://doi.org/10.1007/s10055-018-0349-0

Wiskind, C. (2016). LONE WOLF TERRORISM AND OPEN SOURCE JIHAD: AN EXPLANATION AND ASSESSMENT. International Institute for Counter-Terrorism. https://www.ict.org.il/UserFiles/ict-lone-wolf-osint-jihad-wiskind.pdf

Yamin, M. M., Katt, B., & Nowostawski, M. (2021). Serious games as a tool to model attack and defense scenarios for cyber-security exercises. Computers & Security, 110, 1-22. https://www.sciencedirect.com/science/article/pii/S0167404821002741?via%3Dihub

Yitzhak, E. (19/02/2019). Taqiyya, mentir en nombre de Alá | GEES. Grupo de Estudios Estratégicos. Fecha de consulta (02/03/2023) http://www.gees.org/articulos/taqiyya-mentir-en-nombre-de-ali

Yárnoz, C. (08/01/2015). Doce muertos en un atentado en la revista ‘Charlie Hebdo’ en París. EL PAÍS. Fecha de consulta (25/02/2023) https://elpais.com/internacional/2015/01/07/actualidad/1420629274_264304.html?event_log=go

Zhang, D. (2005). Interactive Multimedia-Based E-Learning: A Study of Effectiveness. American Journal of Distance Education, 19(3), 149-162. https://doi.org/10.1207/s15389286ajde1903_3

Zurro, J. (11/01/2017). El ISIS aprende a hacer propaganda del terror de Hollywood. El Español. Fecha de consulta (30/01/2023) https://www.elespanol.com/series/cine/20170110/184982368_0.html

Álvarez, F. (06/03/2018). Yihadismo para llevar: procesos de radicalización en Occidente. Instituto Español de Estudios Estratégicos. https://www.ieee.es/Galerias/fichero/docs_opinion/2018/DIEEEO24-2018_Yihadismo_Proceso_radicalizacion_FernandoAlvarez.pdf