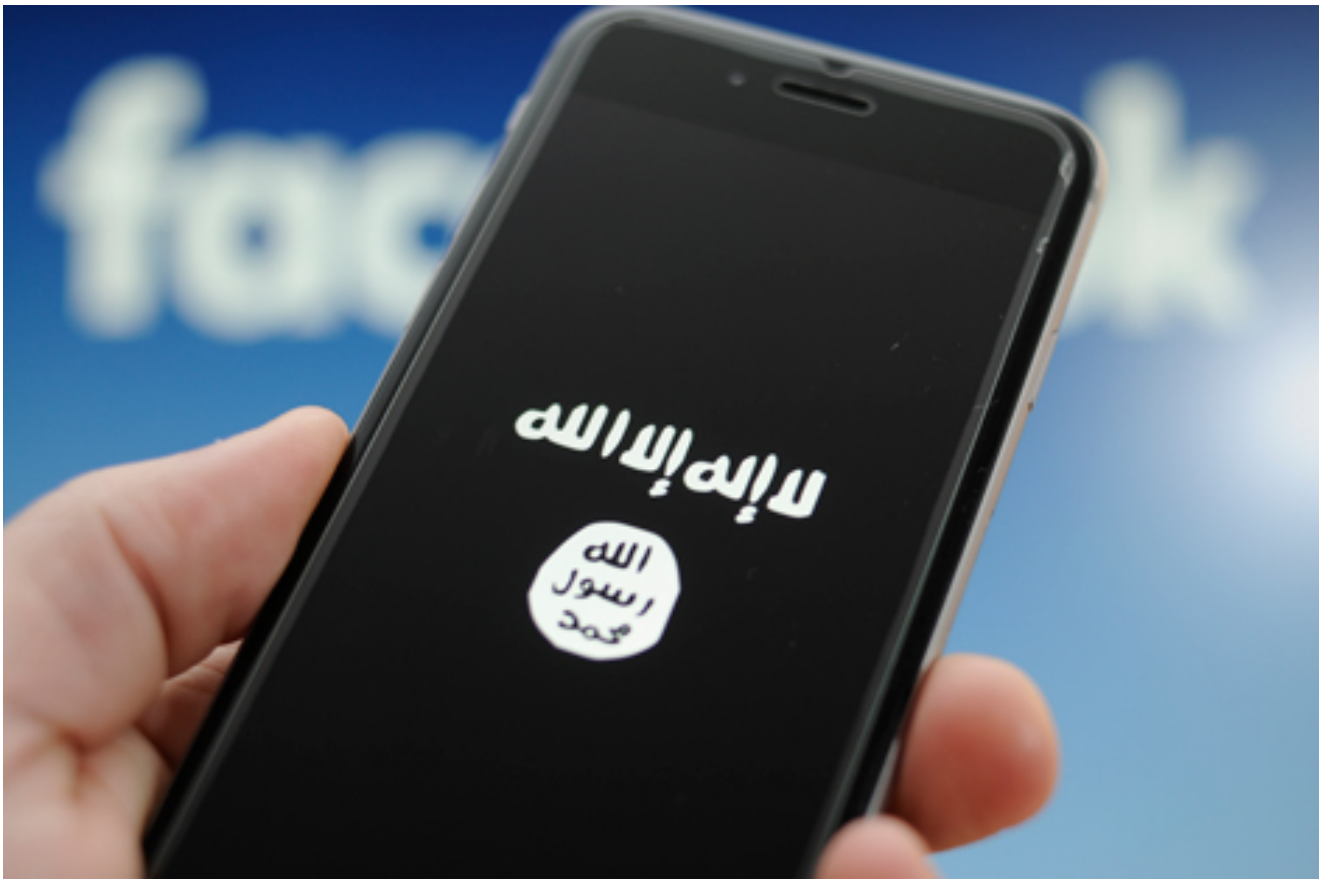
La tecnología del terror: de la dinamita al metaverso

Christina Schoriliang

¿Cómo luchamos contra el uso perverso de las tecnologías emergentes?

Actualmente estamos presenciando una democratización de las tecnologías nuevas y emergentes. En el pasado, las tecnologías avanzadas solo eran accesibles para científicos, funcionarios públicos y militares. Hoy en día, éstas están disponibles como código abierto. Las tecnologías modernas son ubicuas, baratas y fáciles de usar. Y si bien pueden ser un motor para el desarrollo y la prosperidad, también corre el riesgo de ser instrumentalizadas por extremistas que pueden aprovecharse de ella de formas imprevistas y letales.

Nunca en la historia los actores violentos no estatales han estado tan conectados a nivel global, han sido tan habilidosos, dinámicos y tecnológicamente capaces ni han contado con tan buena financiación. Hay tres razones para ello. La primera es que en el pasado la tecnología avanzada estaba solo en manos de unos pocos; hoy, dos tercios del mundo lleva en la mano un *smartphone* que es millones de veces más poderoso que las computadoras de navegación del Apolo 11 que enviaron humanos a la luna en 1969.



La segunda es que las nuevas tecnologías han ampliado enormemente el alcance global de los grupos terroristas, su capacidad para adoctrinar y reclutar instantáneamente sin ningún coste y en relativo anonimato en cualquier parte del mundo. En tercer lugar, los terroristas ahora tienen acceso a tecnología de nivel militar. Gran parte del avance tecnológico es de doble uso, puede utilizarse tanto con fines pacíficos como militares.

La explotación de las tecnologías modernas por parte de actores no estatales se remonta a las últimas décadas del siglo XIX. Durante más de un siglo, los grupos terroristas se han limitado principalmente a dos tipos de armamento: la dinamita y las armas de fuego (sobre todo, el kalashnikov). Poco después de que Alfred Nobel inventara la dinamita en 1867, los movimientos anarquistas compartieron instrucciones sobre su uso, desatando una ola de atentados en más de cincuenta países. El lanzamiento del fusil kalashnikov (AK-47) en la década de 1950 facilitó la segunda ola mundial de violencia política. Utilizados por insurgentes, grupos de crimen organizado, terroristas y “luchadores por la libertad”, estas indestructibles armas siguen matando a un cuarto de millón de personas cada año.

Los actores no estatales, por tanto, siempre han estado interesados ??en obtener y dominar armas innovadoras. Según la “teoría del empoderamiento letal”, las nuevas tecnologías serán rápidamente adoptadas y adaptadas por actores violentos no estatales cuando sean accesibles,

baratas, sencillas de usar, transportables, ocultables y efectivas. A los terroristas les interesan armas que sean útiles en un amplio abanico de contextos: “que magnifiquen los efectos, sean simbólicamente potentes y a las que se les pueda dar usos inesperados”. Por lo tanto, es importante estar atentos a cómo los actores aprovecharán e innovarán nuevas tecnologías con fines maliciosos, con el fin de afrontar las “incógnitas desconocidas” y no repetir los errores basados ??en la “falta de imaginación”, como señala el Informe de la Comisión del 11-S.

Un ejemplo clave es el de los artefactos explosivos improvisados ??(IED en sus siglas en inglés). Entre 2001 y 2006, estos ??fueron responsables del 70% de las bajas en combate en Irak y del 50% en Afganistán. Un estudio riguroso de datos desclasificados sobre IED recopilados entre 2006 y 2014 en Irak y Afganistán demostró que los insurgentes se mantuvieron al día respecto a las costosas medidas tecnológicas empleadas para luchar contra ellos. Los IED se activaban en un principio mediante placas de presión, pero luego se modificaron para que pudieran hacerse estallar con teléfonos móviles. El estudio reveló que los IED tenían las mismas probabilidades de detonar y matar o mutilar en 2014 que en 2006. Además, el uso de IED aumentó en Afganistán de 1.952 en 2006 a 5.616 en 2009.

Estados Unidos dedicó más de 21.000 millones de dólares a la lucha contra los IED, pero los insurgentes se adaptaron con innovaciones sencillas de baja calidad accesibles en el mercado abierto. El fracaso de Estados Unidos en las guerras de Irak y Afganistán se puede atribuir en parte al hecho de que, aunque las fuerzas de defensa estadounidense eran impresionantes, fueron poco eficaces contra las técnicas asimétricas de los actores violentos no estatales contra los que luchaban. Como señaló el general Montgomery Meigs en 2007: “Hay una inversión de tres billones de dólares al año en tecnología de la información… y nuestros oponentes pueden acudir al mercado mundial de tecnologías de la información y obtener en Internet, literalmente gratis, códigos muy sólidos, medios criptográficos, comunicaciones instantáneas o sensores que pueden reutilizar de múltiples maneras”. Ha sido y será cada vez más difícil para las fuerzas armadas convencionales combatir las capacidades tecnológicas de los extremistas y grupos terroristas en la zona gris en la que están operando.

En 1991, la Academia Nacional de Ciencias de EE UU hizo la ahora famosa predicción de que “el terrorista del mañana puede hacer más daño con un teclado que con una bomba”. Internet y las redes sociales, y el *hardware* para acceder a ellas: el *smartphone,* se han convertido en nuevas armas bélicas digitales. Los extremistas han utilizado estas herramientas para llevar a cabo operaciones psicológicas, reclutar, planear y realizar ataques, financiarse y garantizar el anonimato.

Tecnología para operaciones psicológicas

En el siglo V, Sun Tzu escribió que “toda guerra se basa en el engaño”. Hace tiempo que los terroristas comprendieron el poder de las operaciones psicológicas. Osama bin Laden enviaba por fax sus diatribas y sus fetuas a los medios de comunicación. Hoy, la tecnología permite a los terroristas tener un acceso sin precedentes a los ojos y las neuronas de millones de personas a través de Internet y las redes sociales.

Aunque las empresasde redes sociales tienen solo veinte años de existencia, han reconfigurado la vida moderna de modos que son tanto positivos como negativos. Éstas ayudaron a lanzar los movimientos de justicia social #MeToo y BlackLivesMatter. Pero también amplificaron a los grupos extremistas, alimentando movimientos que provocan división social y están basados ??en la raza, el género, la cultura, la política y la religión, incluidos grupos de supremacistas blancos, incels y extremistas salafistas *yihadistas*, entre otros.

El modelo de negocio de las redes sociales se basa en captar la atención para monetizarla. Los algoritmos están diseñados para apelar a la psique humana y actuar como un espejo de nuestros deseos y fascinaciones más profundos. Los creadores de contenido explotan los algoritmos de las plataformas de redes sociales y aprovechan el poder de las emociones humanas dando prioridad al contenido que llama la atención.

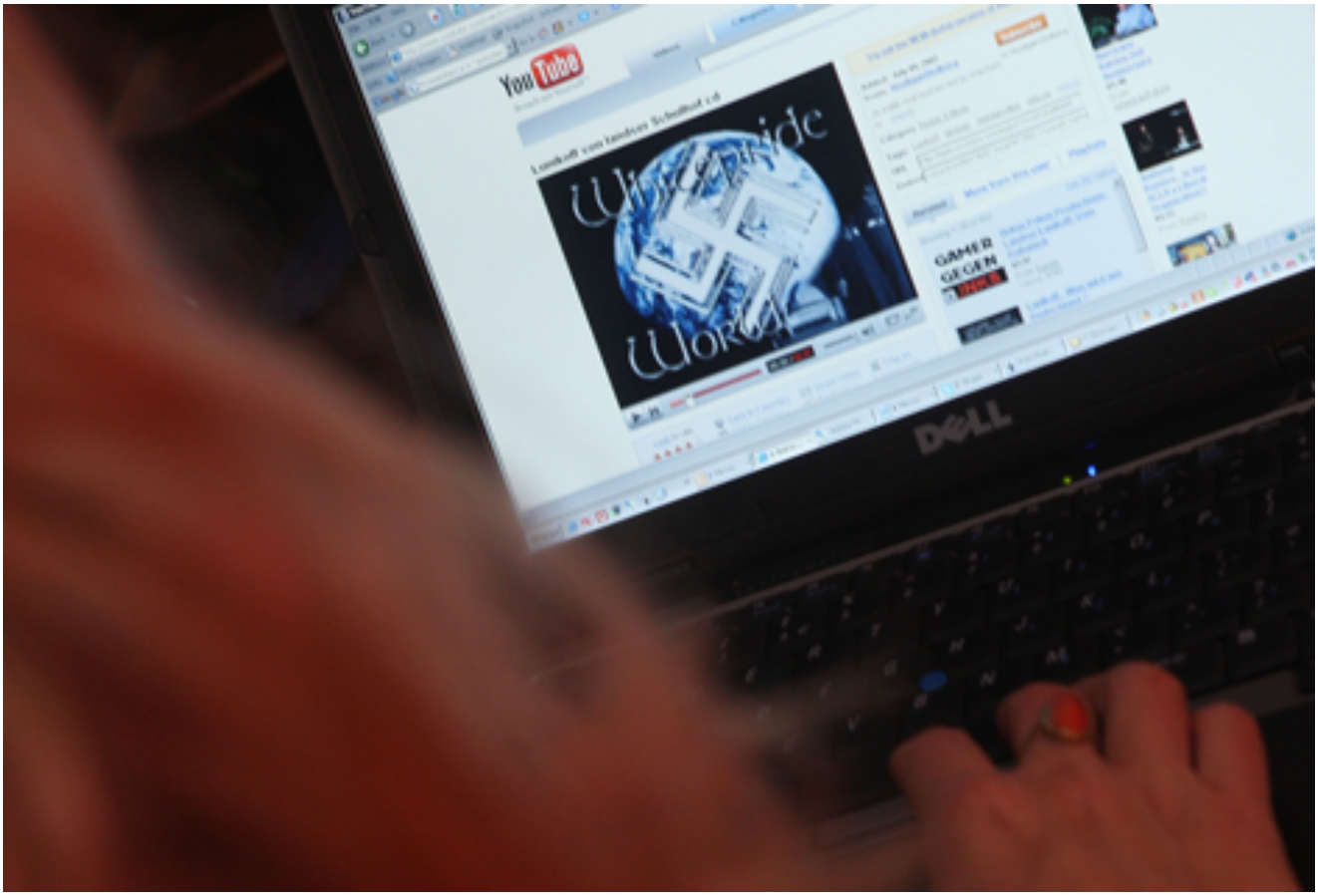
Como resultado, las redes sociales recopilan datos sobre todo y sobre todos, facilitando que distintos grupos se encuentren. Pero lamentablemente también se han convertido en una formidable herramienta para manipular y movilizar a las personas con el fin de cometer delitos, matar, aterrorizar, mutilar, iniciar una insurgencia y ayudar a otros a participar en conflictos e incluso en la guerra. El uso efectivo de las operaciones psicológicas quedó demostrado por la capacidad del Estado Islámico de Irak y el Levante (EIIL) para reclutar en todo el mundo: 41.490 personas de 80 países se afiliaron al EIIL. Algunos fueron tentados por la creencia de que se estaban uniendo a una utopía o a un misión humanitaria, a otros se les prometió estudios de medicina y empleos.

Los terroristas utilizaron a maestros de la manipulación para inspirar y movilizar creando mensajes específicos adaptados al idioma y la cultura correspondientes. Anwar al Awlaki, estadounidense-yemení y destacado propagandista de Al Qaeda en la Península Arábiga (AQAP en inglés), utilizaba Facebook y YouTube para reclutar. Radicalizó a muchos, incluido Umar Farouk Abdulmutallab, quien intentó detonar una bomba en un avión. Este atentado terrorista frustrado justificó ordenar un ataque con drones que finalmente mató a Al Awlaki. Sin embargo, su propaganda sigue siendo incluso más influyente tras su asesinato que antes de su muerte. Entre 2016 y 2020, un total de 89 extremistas occidentales señalaron tener alguna

conexión con él. Su ideología ha sobrevivido, incluida su “44 formas de apoyar la *yihad*”, que se ha propagado *online* como una especie de “mensaje desde la tumba”.

Se utilizan vídeos para aterrorizar a los oponentes, silenciar a la oposición y radicalizar a otros para que se unan. En Afganistán se usan vídeos *snuff,* grabaciones de asesinatos reales, con el fin de enardecer y radicalizar a los afganos para que se conviertan en extremistas, y también se han empleado como advertencia para evitar que los posibles espías o traidores informen tras las líneas enemigas. Los talibanes grababan ataques con IED con móviles y los subían a Twitter para reclutar, recaudar fondos e infundir ánimos. Diseñaron una combinación estratégica de intimidación y ofertas de amnistía para crear la sensación de una victoria inevitable. En agosto de 2021, los mensajes estratégicos de los talibanes basados ??tanto en la coerción como en la persuasión pueden haberlos llevado a conquistar y vencer sin combatir en algunas de las ciudades mejor defendidas de Afganistán.

‘Lobeznos’: reclutando a la siguiente generación de extremistas



Las redes sociales actúan como un amplificador eficaz para atraer a jóvenes ingenuos al

extremismo. En 2016, las plataformas de redes sociales jugaron algún papel en el 90% de los casos de radicalización. En 2018, un informe de investigación que analizó la fuerza de la red del EIIL en Facebook pudo mapear las conexiones entre 1.000 perfiles que apoyaban a este grupo en 96 países, y concluyó que la presencia del EIIL en esta red social era generalizada, profesionalizada y estaba en crecimiento.

Los extremistas de derecha están especialmente interesados ??en reclutar y dar forma a la próxima generación de extremistas. Captan a los jóvenes *online* en los lugares que más frecuentan, como YouTube, Twitch, Steam y DLive. Juntas, estas plataformas acogen a alrededor de 2.250 millones de usuarios al mes, lo que proporciona a los terroristas una enorme base en la que reclutar.

Más de 2.000 millones de usuarios activos visitan YouTube cada mes y ven más de 1.000 millones de horas de vídeos al día. Esto ofrece a los extremistas un extenso campo de reclutamiento; los vídeos que crean brindan apoyo moral, sirven de adiestramiento y animan a quienes los ven a lanzar ataques. Y además incluyen procedimientos paso a paso para construir artefactos explosivos improvisados ??(IED), así como los mejores lugares para colocarlos.

La Red de Sensibilización frente a la Radicalización de la UE (RAN) ha clasificado las plataformas de videojuegos (adyacentes) como “focos” para la radicalización. Twitch es un servicio de emisiones en directo centrado en videojuegos y deportes electrónicos. Tiene un promedio de 30 millones de visitantes diarios, de los cuales un 21% está entre los 13 y los 17 años. Twitch fue lo que utilizó el terrorista que atentó contra una sinagoga en Halle, Alemania, para transmitir en directo su ataque. Steam es la mayor plataforma digital de distribución de juegos para PC, con 120 millones de usuarios mensuales. Contiene juegos que incluyen vivir fantasías extremistas en las que Alemania gana la Segunda Guerra Mundial. Discord, otra plataforma diseñada a medida para usuarios de videojuegos, es una parte importante del ecosistema digital de la extrema derecha. Con más de 140 millones de usuarios mensuales, alberga cientos de servidores privados donde se comparte ideología neonazi, narrativas de extrema derecha y memes que incitan al odio. Los manifestantes de Charlottesville que marcharon bajo el lema “Unite the Right” se conectaron y organizaron a través de los servidores de Discord.

La tecnología inspira el terrorismo de imitación

Los terroristas suscitan respuestas de imitación en todo el mundo. Una serie de ataques

salafistas-*yihadistas* contra objetivos blandos que aterrorizó a ciudades enteras comenzó con el atentado de Niza de junio de 2016, que influyó en el ataque al mercadillo navideño de Berlín en diciembre de ese año y en el atentado de Barcelona de agosto de 2017. En marzo de 2015, otra cadena de atentados terroristas de extrema derecha comenzó con los ataques a dos mezquitas en Christchurch. El perpetrador mató a 51 personas mientras transmitía en directo su ataque mortal en Facebook Live. Durante las primeras 24 horas posteriores al ataque, Facebook eliminó 1,5 millones de copias del vídeo. Inspiró ataques cometidos por imitadores en El Paso, Poway, Baerum, Oslo y Halle. Los terroristas ahora copian un *modus operandi* similar: 1) publican un manifiesto *online*; 2) atacan a un grupo objetivo mientras transmiten en directo por Internet, y 3) publican una recopilación de buenas prácticas, lecciones aprendidas y nuevos llamamientos a la imitación.

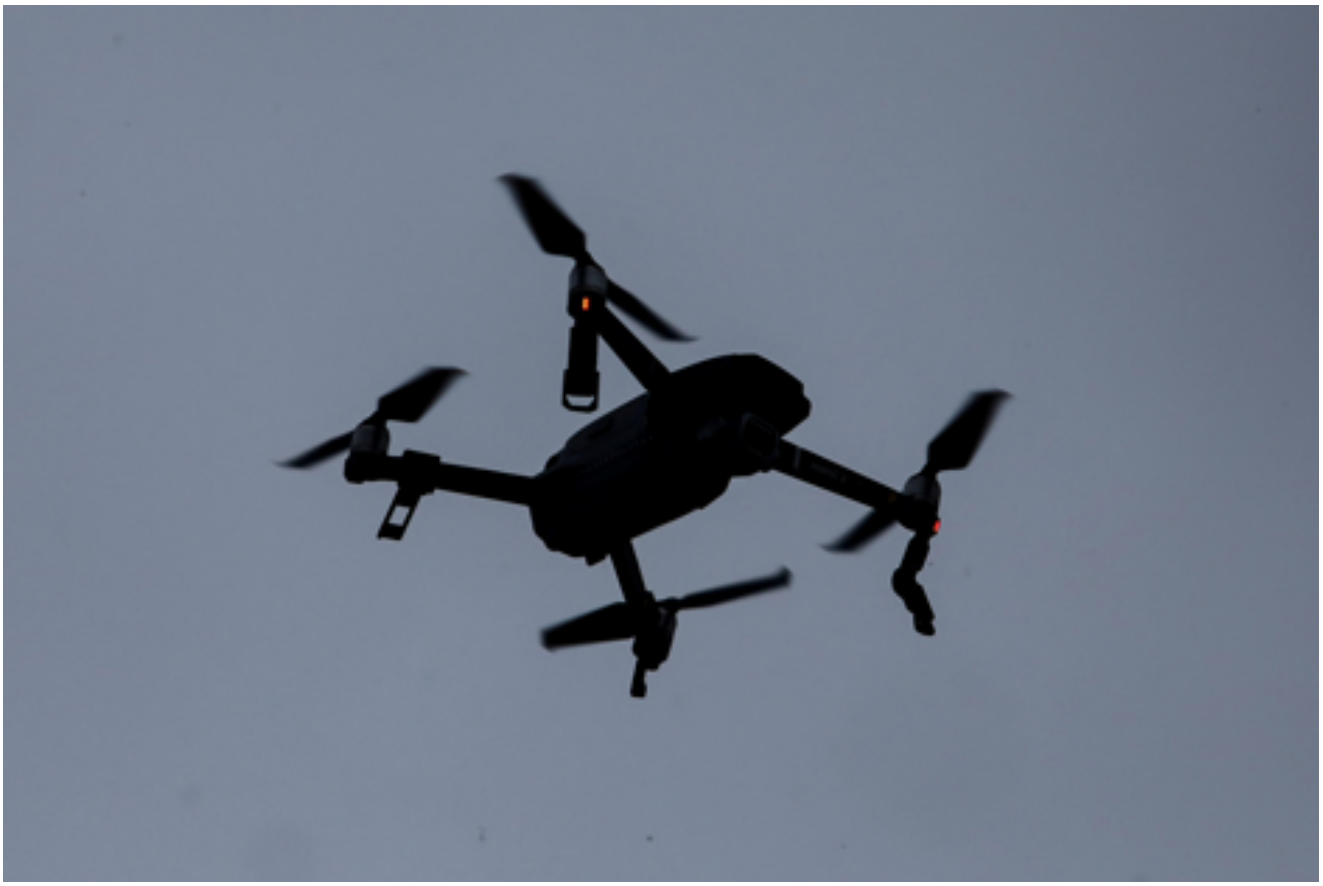
El odio es rentable. Los grupos de supremacistas blancos recaudan fondos monetizando contenidos de odio. Además, *industrializan* sus campañas de recaudación de fondos solicitando criptomonedas. Un informe de FATFMENA sobre el lavado de dinero afirmaba que los terroristas se financiaban a sí mismos usando plataformas como Facebook, YouTube, GoFundMe, Telegram y WhatsApp. Una investigación de *The Times* descubrió que los extremistas —del EIIL y Combat 18— ganaban miles de dólares al mes gracias a la publicidad de grandes marcas que aparecía en sus vídeos más populares, incluyendo empresas muy conocidas como Mercedes Benz y Waitrose.

Tecnología emergentes

Si bien quienes se encargan de diseñar políticas deben contrarrestar el uso de tecnologías existentes por parte de actores no estatales violentos, también deben estar atentos a las tecnologías emergentes. En el pasado, la tecnología militar ha tendido a desarrollarse en un sistema cerrado, mientras que hoy hemos entrado en una etapa de innovación abierta sin precedentes. Los individuos y los grupos privados son libres no solo de comprar estas tecnologías, usarlas y distribuirlas, sino también de inventarlas y darles nuevos usos. Ya en 2008, el grupo Lashkar e Taiba atacó Bombay durante 36 horas gracias a 10 extremistas que fueron capaces de planificar, coordinar y llevar a cabo su misión utilizando dispositivos avanzados, incluyendo GPS y teléfonos móviles con los que obtenían información de la situación en tiempo real. Marcó una nueva modalidad de guerra urbana caracterizada por ataques simbólicos, objetivos múltiples y un gran número de víctimas, que dio como resultado más de 170 muertos, mientras que los heridos superaron los 300. Este suceso demostró la rapidez con la que las nuevas tecnologías como el GPS pueden utilizarse para fines perversos

Impresión 3D. Hoy las tecnologías emergentes son accesibles para los extremistas que siguen activamente los espacios de *hackers*. Unos estudiantes usaron tecnología de impresión 3D para construir un dron que combinaron con el sistema de navegación de un teléfono Android que le permitió volar sin un caro sistema de navegación y compartieron sus hallazgos. En 2020, un terrorista alemán de extrema derecha en Halle usó manuales *online* y una impresora 3D para imprimir partes de su arma, todo con un gasto de 50 dólares. El intento fracasó pero su objetivo era demostrar la viabilidad de las armas improvisadas.

Vehículos autónomos. En el futuro, estos automóviles podrían dar lugar a múltiples escenarios de ataques maliciosos, incluida la replicación de los atentados mortales con vehículos llevados a cabo en 2016 y 2017 en Barcelona, ??Berlín, Londres, Nueva York, Niza y Estocolmo. En 2011, Ansar al Islam construyó un automóvil sin conductor con ametralladoras a control remoto. En 2016, el EIIL convirtió un coche en un arma a control remoto con un calefactor para simular la presencia de vida.



Drones. En 2011, un simpatizante de Al Qaeda intentó usar un avión teledirigido cargado de granadas para bombardear el Capitolio de Estados Unidos. Desde 2016, el EIIL ha estado utilizando drones para llevar a cabo misiones de inteligencia, vigilancia y reconocimiento. Este grupo realizó ataques con estos aviones no tripulados que transportaban explosivos, y formó

una unidad de “Drones de los muyahidines”. Inmovilizó a las fuerzas de seguridad iraquíes durante un período de 24 horas en Siria ejecutando 70 misiones con este tipo de tecnología.

En noviembre de 2021, se utilizaron cuadricópteros teledirigidos cargados de explosivos para intentar asesinar al primer ministro iraquí, Mustafa al Kadhimi, en su casa. El ataque demostró que los actores no estatales armados pueden usar drones para infundir terror y provocar cambios políticos. Los recientes ataques con ellos atribuidos al movimiento Houthi en Yemen, en los que participaron varios drones en vuelos de largo alcance, también indican cómo los actores no estatales violentos actuarán en el futuro. En 2026, más de un millón de este aviones no tripulados repartirán pedidos de compras, creando nuevas vulnerabilidades. El Foro Global contra el Terrorismo publicó el Memorando de Berlín sobre buenas prácticas para contrarrestar el uso terrorista de sistemas aéreos no tripulados.

Inteligencia Artificial. La IA tendrá un gran impacto en la seguridad y es la tecnología de doble uso por excelencia. La inteligencia artificial puede beneficiar a los terroristas dándoles acceso a productos de alta tecnología ampliamente disponibles. Estos incluyen el lanzamiento de *slaughter bots*, vehículos autónomos que lancen explosivos en ataques rápidos y coordinados. Todos los componentes para crearlos están disponibles y se pueden adquirir listos para usar. La IA potencialmente permitirá que los adversarios actúen con microprecisión, pero a macroescala y con mayor velocidad. Esta tecnología mejorará los ciberataques y las campañas de desinformación digital y puede usarse contra los jóvenes vulnerables de múltiples y novedosas maneras.

El metaverso es un mundo de realidad virtual caracterizado por una experiencia tridimensional y multisensorial. Para los terroristas puede ser una manera de expandir su arsenal. Hoy, alguien interesado en hablar sobre “cultura del asedio”, una ideología neonazi, probablemente tendrá que leer sobre ella en el sitio web Siege Culture, que posiblemente ya no esté disponible *online.* En el metaverso, la gente puede encontrarse con el autor de *Siege,* el neonazi James Mason, o su doble de IA. El metaverso también puede resucitar a Anwar Al Awlaki o a Osama bin Laden, propagando aún más sus ideologías extremistas. La coordinación de los ataques será más fácil cuando los extremistas puedan realizar misiones preventivas de reconocimiento en el mundo virtual antes de realizar los ataques físicos.

El camino a seguir

Combatir el uso perverso de las nuevas tecnologías no es fácil. La tecnología de encriptación protege a los terroristas de los intentos de las empresas de eliminarlos de las redes sociales. La

difusión de tecnologías de doble uso seguirá empoderando a los extremistas. Por lo tanto, es importante hacer cumplir la regulación, como se hizo para reducir las bombas con dinamita en Europa, y abordar las causas sociales que impulsan a los extremistas a cometeratentados, como se hizo en EE UU a principios del siglo XX.

También es fundamental informar al público de los nuevos riesgos, tal como hizo en 2022 el Departamento de Seguridad Nacional de Estados Unidos (DHS) cuando advirtió que grupos extremistas en el interior del país habían desarrollado planes creíbles y específicos para atacar la red eléctrica. También se han producido advertencias similares sobre ataques de *ransomware* contra infraestructura crítica por parte de Australia, Estados Unidos y el Reino Unido.

Una de las mayores prioridades es inmunizar a los jóvenes en este sentido advirtiéndoles sobre la naturaleza subversiva de Internet y las redes sociales. Esto deberá integrarse en las políticas educativas, que pueden dedicar recursos a la “ciudadanía digital” y al uso crítico de las redes sociales, así como diseñar planes de acción nacionales para prevenir el extremismo violento. Al mismo tiempo, es importante trabajar en sintonía con los cinco grandes *gigantes* tecnológicos para crear asociaciones público-privadas. Su valor de mercado combinado de 9,3 billones de dólares les concede suficientes recursos para contribuir a crear una Internet que promueva los valores democráticos en lugar de destruirlos.

Como presenciamos en la primera ola de terrorismo moderno, la invención de la dinamita por parte de Nobel rápidamente dejó salir al genio de la botella, por así decirlo, con la creación de 125 variedades diferentes de ella. Esto se sumó a las reticencias de los gobiernos a la hora de poner límites y regularla. La comunidad global debe encontrar mejores respuestas y desarrollar un mayor conocimiento de la guerra irregular y psicológica. Los conflictos recientes han demostrado que los ejércitos profesionales carecen de la agilidad operativa acorde con su tamaño y adiestramientoen un panorama de amenazas a la seguridad que están siendo promovidas por actores violentos no estatales, criminales, extremistas, piratas informáticos, blogueros y youtubers que han sabido aprovechar con éxito la tecnología para lograr sus objetivosestratégicos.

En Estados Unidos, dos décadas de “guerra contra el terror” y el endurecimiento de sus defensas internas han generado consecuencias inesperadas, incluido un aumento del extremismo a nivel nacional y del malestar social. La exposición de las personas a la incitación a través de la web ha causado una infección generalizada de resentimiento, desinformación y teorías de la conspiración que está creando ciclos de ira que debilitan no solo al país, sino también a las democracias de todo el mundo. El público en general ha perdido la confianza en el gobierno y en su capacidad para imponer la ley y el orden, y la pandemia global está

echando más leña al fuego.

Los Estados se enfrentan ahora a uno de los mayores dilemas en lo que se refiera a la lucha contra el terrorismo: diseñar medidas antiterroristas eficaces y, al mismo tiempo, preservar los valores democráticos liberales. La comunidad que trabaja en temas de seguridad debe despertar ante el desafío que plantean las tecnologías emergentes, especialmente las digitales. Aunque Internet y las redes sociales parecen mucho más inofensivas que la dinamita, podrían considerarse la dinamita social de esta generación.

Fecha de creación
16 marzo, 2022