

Capítulo 12

Ciberdisidencia y terrorismo digital: análisis del hacktivismo y el ciberterrorismo en la era posmoderna*

DOI: <https://doi.org/10.25062/9786287818729.12>

Carlos Enrique Álvarez Calderón

Escuela Superior de Guerra "General Rafael Reyes Prieto"

Resumen: Este capítulo analiza el *hacktivismo* y el ciberterrorismo en el contexto de los conflictos digitales del siglo XXI; examina su evolución desde formas tempranas de desobediencia simbólica hasta su integración en redes descentralizadas y automatizadas de insurgencia digital; establece una periodización en seis fases que refleja su transformación en respuesta a las lógicas tecno-políticas contemporáneas, y conceptualiza el ciberterrorismo como una categoría estratégica difusa, a empaquetar desde ataques a infraestructuras críticas hasta la propaganda viral y el reclutamiento mediante plataformas encriptadas. Los estudios de caso de ISIS, Hezbolá y actores estatales revelan cómo el ciberterrorismo opera como componente clave en las guerras híbridas y de percepción. Se destaca la falta de una tipificación normativa del ciberterrorismo en el derecho colombiano, lo cual limita la capacidad de respuesta estatal. Finalmente, se propone fortalecer el rol del Comando Conjunto Cibernético como eje doctrinal y estratégico frente a esta amenaza.

Palabras clave: ciberseguridad; ciberterrorismo; guerra de quinta generación; *hacktivismo*.

* Capítulo de libro resultado del proyecto de investigación "Desafíos y nuevos escenarios de la seguridad multidimensional a nivel nacional, regional y hemisférico en el decenio 2015-2025", del grupo de investigación Centro de Gravedad, de la ESDEG, categorizado A por MinCiencias y registrado con el código COL0104976. Los puntos de vista pertenecen a los autores y no necesariamente reflejan el pensamiento de las instituciones participantes.

Carlos Enrique Álvarez Calderón

Candidato a doctor en Estudios Estratégicos, Seguridad y Defensa, Escuela Superior de Guerra "General Rafael Reyes Prieto", Colombia. Magíster en Coaching Ontológico Empresarial, Universidad San Sebastián, Chile. Politólogo y Magíster en Relaciones Internacionales, Pontificia Universidad Javeriana, Colombia. Investigador Asociado MinCiencias y Docente Investigador, Escuela Superior de Guerra "General Rafael Reyes Prieto". Profesional Oficial de Reserva, Fuerza Aeroespacial Colombiana. Asesor y consultor en seguridad y defensa para instituciones de las Fuerzas Militares de Colombia y a nivel internacional.

<https://orcid.org/0000-0003-2401-2789> - Contacto: carlos.alvarez@esdeg.edu.co

Citación APA: Álvarez Calderón, C. E. (2026). Ciberdisidencia y terrorismo digital: análisis del hacktivismo y el ciberterrorismo en la era posmoderna. En C. E. Álvarez Calderón (Ed.), *El campo de batalla digital: la defensa nacional en la era algorítmica, Volumen III. (Armas de la mente: guerra memética y manipulación informativa en la quinta generación de la guerra)*(pp. 1053-1132). Sello Editorial ESDEG.
<https://doi.org/10.25062/9786287818729.12>

EL CAMPO DE BATALLA DIGITAL: LA DEFENSA NACIONAL EN LA ERA ALGORÍTMICA

VOLUMEN III. ARMAS DE LA MENTE: GUERRA MEMÉTICA Y MANIPULACIÓN INFORMATIVA EN LA QUINTA GENERACIÓN DE LA GUERRA

ISBN IMPRESO (Obra completa): 978-628-7818-65-1

ISBN DIGITAL (Obra completa): 978-628-7818-69-9

ISBN IMPRESO Volumen I: 978-628-7818-68-2

ISBN DIGITAL Volumen I: 978-628-7818-72-9

DOI: <https://doi.org/10.25062/9786287818729>

Colección Seguridad y Defensa

Sello Editorial ESDEG

Escuela Superior de Guerra "General Rafael Reyes Prieto"

Bogotá D.C., Colombia

2026



Introducción

El ciberespacio es hoy tanto un escenario de resistencia política como un teatro de subversión cognitiva. En él conviven formas de activismo que buscan emancipar la conciencia (ciberdisidencia), con estrategias que pretenden capturarla (terrorismo digital). Ambas expresan una disputa por la información, la emoción y la percepción, donde los algoritmos y las redes sociales se han convertido en los nuevos intermediarios del poder. La digitalización de la vida social no solo transformó la manera en que los ciudadanos se informan y se movilizan, sino también la forma en que los Estados, las corporaciones y los actores subversivos intervienen en la mente colectiva.

En este entorno hiperconectado, el conflicto ya no se libra únicamente por territorios físicos, sino por territorios cognitivos, donde la atención, la credibilidad y la memoria son recursos estratégicos. En tal contexto, la ciberdisidencia aparece como una expresión legítima de libertad en el espacio digital, mientras que el ciberterrorismo representa su degeneración extrema: la manipulación planificada de las creencias y emociones para generar caos, miedo o sumisión. Este capítulo examina esa tensión entre emancipación y control, mostrando cómo el frente cibercognitivo se ha convertido en el eje estructurante de las nuevas formas de conflicto político e informacional del siglo XXI.

En las dos primeras décadas del siglo XXI, el ciberespacio ha evolucionado de una infraestructura tecnológica neutral a un escenario polémico de disidencia política, disputa ideológica y violencia estratégica. Dejando de ser una mera herramienta de comunicación o comercio, el ámbito digital se ha convertido en un entorno donde movimientos sociales, agencias estatales y actores extremistas se involucran en dinámicas y complejas luchas por la influencia, la legitimidad y la disrupción. Por consiguiente, este capítulo explora la pregunta central de

investigación: ¿En qué punto la resistencia digital se convierte en violencia digital, y cómo puede distinguirse conceptual y éticamente entre *hacktivismo* y ciberterrorismo en el panorama digital posmoderno?

El propósito de este capítulo es analizar cómo el ciberespacio funciona como un dominio de doble uso, al empoderar a los actores de la sociedad civil para desafiar la injusticia y, al mismo tiempo, ofrecer herramientas y anonimato a quienes ejercen la coerción y el terrorismo digitales. A partir de literatura interdisciplinaria sobre estudios de seguridad, teoría de los medios y sociología digital, este capítulo describe la evolución del ciberespacio como un espacio de protesta y amenaza asimétrica, analiza el papel de condiciones posmodernas como la descentralización y el poder simbólico, y propone un marco espectral para categorizar la acción política digital, desde la desobediencia civil hasta el ciberterrorismo. Con ello, busca aclarar la ambigüedad conceptual que rodea la contienda digital y contribuir a una comprensión más matizada de las implicaciones éticas y estratégicas de la ciberguerra y la guerra cognitiva.

En los últimos años, el ciberespacio ha empoderado a una amplia gama de actores políticos, en particular a entidades no estatales, para participar en formas de resistencia que antes eran inaccesibles debido a limitaciones logísticas, geográficas o institucionales. Como destacan Jordan y Taylor (2004), el auge del *hacktivismo*, al que definen como la fusión de técnicas de *hacking* con activismo político o ideológico, ejemplifica cómo las redes digitales han permitido la convergencia de la habilidad técnica y la intención política. Estos actos, que abarcan desde las desfiguraciones simbólicas hasta las interrupciones masivas como las campañas de Denegación de Servicio Distribuido (DDoS), desafían las nociones tradicionales de protesta política, al explotar la arquitectura informativa de la propia sociedad (Sauter, 2014).

No obstante, el ciberespacio también se constituye en un terreno fértil para una variedad de amenazas asimétricas, como el ciberterrorismo y otras operaciones híbridas que difuminan la línea entre el arte de gobernar y la subversión. Denning (2007) define el ciberterrorismo como ataques con motivación política a sistemas digitales que resultan, o amenazan con resultar, en violencia o interrupciones generalizadas. Estos actos no se limitan al sabotaje de infraestructuras, sino que también pueden incluir las operaciones psicológicas, la difusión de propaganda y la facilitación digital de la violencia cinética. Entonces, la presencia de estas amenazas en el mismo espacio comunicativo que la disidencia legítima plantea un dilema conceptual, y es ¿cómo pueden las sociedades democráticas garantizar la

protección de las libertades civiles en el ciberespacio y, al mismo tiempo, mitigar los riesgos que plantean quienes lo utilizan como arma para el terrorismo?

Como demostrará este capítulo, el auge de la contienda digital refleja dinámicas posmodernas más amplias, caracterizadas por la descentralización de actores, la política simbólica y la ambigüedad ontológica. Los límites entre protesta y guerra, entre civiles y combatientes, entre disidencia legal y disrupción ilegal son cada vez más difíciles de delinear en un mundo donde el código, las imágenes y las narrativas pueden tener efectos estratégicos similares a los del uso de la fuerza convencional, es decir, cinética, militar y letal (Karatzogianni, 2015; Montasari, 2023). Por lo tanto, el campo de batalla digital no es una mera metáfora: es una realidad material y simbólica que exige un análisis teórico y una reflexión política minuciosos.

La condición posmoderna de la guerra y el activismo se define por el colapso de las binariedades tradicionales de la guerra/paz, combatiente/civil, público/privado. En el ciberespacio, este colapso es particularmente agudo. A diferencia de los campos de batalla tradicionales, donde los combatientes son identificables y los enfrentamientos están geográficamente delimitados, los conflictos digitales involucran a actores dispersos y anónimos que a menudo operan fuera o por debajo del radar estatal (Karatzogianni, 2015). Estos actores pueden ser individuos, redes, bots o conjuntos híbridos, y sus acciones suelen resonar tanto en el ámbito de la percepción como en el mundo físico.

La descentralización, un rasgo distintivo de los movimientos digitales, potencia y dificulta la resistencia. La lógica de la sociedad en red, como la describe Castells (2009), facilita la formación de colectivos *ad hoc*, orientados a objetivos, que pueden movilizarse con rapidez y a nivel global. Este modelo de protesta "enjambre", que es evidente en las campañas DDoS de grupos hacktivistas, altera las formas jerárquicas de poder mediante una organización fluida y horizontal (Sauter, 2014). Sin embargo, esta falta de estructura también impide la rendición de cuentas y la coherencia de los mensajes, creando ambigüedades en torno a la responsabilidad y la intención.

El poder simbólico, ejercido mediante la apropiación y manipulación de señales y narrativas digitales, desempeña un papel fundamental en las guerras cognitivas. Como argumentan académicos como von Busch y Palmås (2006), el hacktivismo opera menos mediante la destrucción que mediante la construcción, ya que reconfigura el significado, reclama el espacio digital y desafía el discurso dominante. Los memes digitales, las filtraciones y el contenido viral se convierten

en armas de subversión, difuminando la línea entre la expresión política y la guerra psicológica. Y la erosión de los límites se extiende también a los ámbitos legal y ético. Las acciones hacktivistas a menudo violan las leyes relativas al acceso no autorizado, pero reclaman legitimidad apelando a la desobediencia civil o a principios morales superiores. Los gobiernos, a su vez, despliegan cada vez más vigilancia digital y capacidades cibernéticas ofensivas, a menudo bajo justificaciones legales opacas. En esta zona gris, definir la delincuencia, la protesta y el terrorismo se convierte en un acto político en sí mismo.

Por consiguiente, comprender la contienda digital requiere un modelo de espectro que abarque tanto la desobediencia civil no violenta como el extremismo violento. En un extremo, acciones como las peticiones digitales, los boicots en línea o las protestas DDoS están diseñadas para generar disrupción simbólica, llamando la atención sobre las causas y minimizando el daño. Estas formas de ciberdisidencia evocan la tradición de la desobediencia civil, adaptada a las posibilidades de internet (Jordan, 2002; Sauter, 2014).

En el centro del espectro se encuentran actos que pueden implicar daños a la propiedad, robo de datos o acceso ilegal, como por ejemplo, la exposición de documentos confidenciales o el hackeo de servidores gubernamentales. Estas tácticas, si bien no son letales, a menudo provocan fuertes respuestas estatales, así como controversia pública. Las actividades de WikiLeaks, por ejemplo, ponen de relieve las tensiones entre la transparencia, la seguridad y la rendición de cuentas. En el extremo opuesto del espectro se encuentra el ciberterrorismo, que consiste en ataques que buscan infundir miedo, causar perturbaciones en infraestructuras críticas o apoyar el terrorismo cinético. Si bien el ciberterrorismo a gran escala sigue siendo poco frecuente, algunos actores como el Estado Islámico (ISIS) y Hezbolá han demostrado usos sofisticados del ciberespacio para el reclutamiento, la propaganda y la planificación operativa (Ganor, 2015; Koops, 2016).

La dificultad para distinguir estas categorías radica no solo en las herramientas y plataformas compartidas que se utilizan, sino también en la mutabilidad de los actores, ya que un activista digital hoy puede radicalizarse mañana. Además, los Estados pueden etiquetar la disidencia como terrorismo con fines estratégicos, como se observa en la criminalización de grupos hacktivistas o la represión de los movimientos de protesta digitales bajo las leyes antiterroristas (Karagiannopoulos, 2018). La flexibilidad de los límites entre categorías exige un análisis contextual que considere la intención, el método y el impacto.

En el corazón del campo de batalla cibernético se encuentra un dilema conceptual y ético: ¿cuándo la resistencia digital se convierte en violencia digital? La respuesta se centra en cuestiones de intención, proporcionalidad y la naturaleza del daño; si bien las definiciones tradicionales de violencia enfatizan las lesiones físicas o la muerte, en el ámbito digital el daño puede ser psicológico, simbólico o económico. La filtración de datos privados puede no matar, pero puede destruir vidas. La manipulación del discurso en línea mediante comportamientos inauténticos coordinados puede no vulnerar las redes, pero puede erosionar los procesos democráticos. Por lo tanto, la violencia digital debe entenderse en términos más amplios que reflejen las realidades del poder en red.

Además, la intención es notoriamente difícil de determinar en el ciberespacio. La atribución sigue siendo un desafío persistente, lo que permite una negación plausible y complica la respuesta legal o militar (Jarvis et al., 2014). Un ataque DDoS puede ser una protesta, una broma o un precursor de un ciberataque, según el contexto y la identidad del actor. Esta ambigüedad crea un espacio donde los actores estatales y no estatales maniobran estratégicamente, a menudo desafiando los límites éticos.

La legitimidad moral de las tácticas digitales se cuestiona aún más. Para algunos, el hacktivismo es una forma necesaria de resistencia contra sistemas injustos, similar al sabotaje y las interrupciones de las luchas anticoloniales o antiautoritarias (Burnett & Vescina, 2017). Para otros (Denning, 2007; Ganor, 2015; Montasari, 2023), incluso las interrupciones digitales no violentas amenazan el Estado de derecho y la seguridad pública. Por lo tanto, enmarcar las acciones como disidencia legítima o amenaza criminal es profundamente político, moldeado por el control narrativo y el poder institucional. En última instancia, el campo de batalla digital obliga a replantear la resistencia, el poder y la violencia; a medida que se redibuja la línea entre protesta y terror en el ciberespacio, las sociedades deben lidiar con las implicaciones éticas, legales y estratégicas de esta transformación. Por ende, equilibrar la protección de los derechos fundamentales con la necesidad de seguridad, así como lograr distinguir entre disidencia simbólica y violencia coercitiva, serán desafíos centrales para abordar el futuro de los ciberconflictos.

Hactivismo e ideologías de la ciberdisidencia

El hacktivismo, fusión de los términos *hacking* y activismo, se refiere en principio al uso de herramientas, tácticas y cultura digitales para participar en la protesta y

la disidencia política. Se sitúa en la controvertida intersección del ingenio tecnológico, la desobediencia civil y la política disruptiva, por lo que desde su conceptualización en la última década del siglo XX, el hacktivismo se ha convertido en una forma global y cada vez más visible de resistencia digital.

El *activismo*, definido generalmente como la práctica de emprender acciones directas u organizadas para alcanzar objetivos políticos, sociales o económicos, ha experimentado una importante evolución conceptual con el auge del entorno digital. En la literatura académica, el activismo se entiende alternativamente como confrontación, comunicación, resistencia simbólica o participación en red. Las definiciones tradicionales, basadas en la lógica de la desobediencia civil y la teoría de los movimientos sociales, consideran el activismo como una acción colectiva organizada destinada a desafiar el poder institucional. Jordan (2002) concibe el activismo como “cualquier actividad que se realiza para transformar la sociedad” (p. 17), enfatizando su carácter confrontativo y moral, e incluye la “acción directa” y la “desorganización”, destacando la interacción entre la espontaneidad popular y el propósito estratégico (Jordan, 2002, pp. 53-55).

En este orden de ideas, Jordan y Taylor (2004) argumentan que el hacktivismo representa un nuevo tipo de activismo que fusiona el conocimiento técnico con la protesta política, ampliando así el alcance de las tácticas activistas más allá de los repertorios tradicionales. Desde una perspectiva centrada en los medios, Karatzogianni (2015) define el activismo digital como la “participación política, actividades y protestas organizadas en redes digitales más allá de la política de representación” (p. 1). Su tipología de las cuatro olas del activismo digital sitúa el activismo dentro de cambios más amplios en la política global con relación a la información, señalando cómo los movimientos posteriores a 2010, como WikiLeaks, la Primavera Árabe y *Occupy*, desdibujaron las fronteras entre el periodismo, la protesta social y la guerra cognitiva. Karatzogianni (2015) sitúa el activismo digital no solo como una resistencia reaccionaria, sino como una fuerza formativa dentro de la gobernanza en red y la política de identidades.

Por consiguiente, el hacktivismo representa una ruptura radical con las formas convencionales de protesta al convertir el código en un medio de resistencia. Según Coleman (2014), el hacktivismo es “el uso no violento de herramientas digitales ilegales o legalmente ambiguas para la consecución de fines políticos” (p. 63). Para Sauter (2014), las intervenciones activistas, como los ataques DDoS, deben interpretarse no solo como interrupciones, sino como actos simbólicos

análogos a las sentadas o los bloqueos, haciendo hincapié en las dimensiones comunicativas y performativas del activismo en el ciberespacio.

Otros académicos añaden matices ideológicos a estas definiciones; por ejemplo, von Busch y Palmås (2006) distinguen entre el *cracktivismo* destructivo y el hacktivismo abstracto constructivo, enmarcando el activismo como un esfuerzo por construir imaginarios políticos alternativos en lugar de simplemente oponerse a las estructuras existentes. De manera similar, Burnett y Vescina (2017) abordan el activismo desde la perspectiva de la privacidad digital, caracterizando el hacktivismo como una resistencia al capitalismo de vigilancia y la mercantilización de datos.

En estas definiciones, surgen tensiones clave: el activismo como disrupción versus construcción, como simbolismo versus estrategia, y como resistencia descentralizada versus cooptación institucional. En un contexto digital, el activismo ya no es dominio exclusivo de los manifestantes visibles en la calle, sino también de programadores anónimos, filtradores de datos y estrategias de memes digitales. Por lo tanto, la evolución del activismo no es solo técnica, sino ontológica: está redefiniendo lo que se considera acción política en un mundo en red.

En este contexto, el hacktivismo puede definirse ampliamente como el uso con motivaciones políticas de herramientas y técnicas de *hacking* para influir o interrumpir las infraestructuras de comunicación digital. Estas incluyen tácticas como la desfiguración de sitios web, ataques de denegación de servicio distribuido (DDoS), filtraciones de datos e intrusiones en la red, sin ánimo de lucro, sino para expresar disidencia o protestar (Jordan & Taylor, 2004). Si bien la terminología se popularizó en la segunda mitad de la década de 1990 gracias a grupos como el *Cult of the Dead Cow*, sus raíces se encuentran en subculturas *hacker* anteriores que valoraban el acceso abierto, la descentralización y la subversión tecnológica (Karatziogianni, 2015).

En consecuencia, el hacktivismo no sería simplemente la traducción digital de la protesta callejera; refleja las posibilidades, la lógica y el lenguaje de la esfera digital en red; en efecto, Jordan y Taylor (2004) enfatizan que el hacktivismo se nutre de una tradición de acción directa, pero la reconfigura dentro de las condiciones de la cibercultura, donde la visibilidad, la replicación y la disrupción simbólica prevalecen sobre la confrontación física.

Evolución del hacktivismo

Karatzogianni (2015) ha propuesto un modelo que traza la evolución del activismo digital (y, por extensión, del hacktivismo), a lo largo de cuatro olas políticas distintas. Cada ola refleja un contexto histórico, tecnológico e ideológico particular en el que surgió y se desarrolló la resistencia digital. En este sentido, la primera fase (1994-2001) surgió tras la creación de la *World Wide Web* y se caracterizó por visiones utópicas de la democracia digital. Los primeros actos hacktivistas fueron principalmente simbólicos, con el objetivo de expresar disidencia o llamar la atención sobre causas sociales.

La participación en línea del Ejército Zapatista de Liberación Nacional (EZLN) en 1994, facilitada por el Teatro de Disturbios Electrónicos (TDE)¹ y su herramienta FloodNet², representa un momento crucial en la acción directa virtual masiva. FloodNet y el TDE marcaron un hito porque introdujeron el concepto de acción directa digital dentro del campo del activismo, establecieron un precedente para el uso de herramientas digitales como expresión artística y política, y abrieron el debate ético y legal sobre si este tipo de protestas debían considerarse manifestación legítima o ataque cibernético.

Como lo explican Jordan y Taylor (2004), las acciones del TDE demostraron cómo los medios digitales podían ser empleados para simular tácticas de desobediencia civil sin infringir físicamente los espacios, redefiniendo el campo de lo político en la era de internet. Otros ejemplos tempranos incluyen la formación de IndyMedia durante las protestas antiglobalización de Seattle (1999), y las desfiguraciones simbólicas de sitios web por parte de los Electrohippies y RTMark; estas

¹ El TDE (Electronic Disturbance Theater) es un colectivo de arte activista fundado en 1997 en Estados Unidos por un grupo de artistas y tecnólogos, entre los que se destacan Ricardo Domínguez, Carmin Karasic, Brett Stalbaum y Stefan Wray. Este colectivo es considerado uno de los pioneros del hacktivismo. Surge como respuesta a las luchas del movimiento zapatista en México y como crítica a las estructuras globales de poder, en particular aquellas ejercidas por los gobiernos y las corporaciones a través de las redes digitales; su objetivo era generar formas de protesta simbólica en el ciberespacio, utilizando el arte y el *software* como medios de acción política. En lugar de sabotaje o destrucción, el TDE promovía la acción directa digital no violenta, comparándola con tácticas clásicas como los "sitins" (sentadas) de los movimientos por los derechos civiles.

² FloodNet fue la herramienta más emblemática desarrollada por el TDE. Es un programa basado en Java que permitía a los usuarios participar en protestas digitales enviando múltiples solicitudes automáticas a servidores web específicos, con el objetivo de: 1) saturar el sitio web del objetivo (gobiernos, instituciones militares, corporaciones); 2) hacer visibles los reclamos mediante la inserción de mensajes simbólicos en los campos de búsqueda del servidor; y 3) simular una sentada virtual, donde miles de personas "ocupaban" simbólicamente un espacio digital al igual que una plaza física. El primer uso destacado de FloodNet ocurrió en apoyo al EZLN, dirigiendo las acciones contra sitios del Gobierno mexicano en 1998; los participantes simplemente accedían a una página web provista por el TDE, y el script comenzaba a enviar repetidas solicitudes al objetivo, reproduciendo el efecto de una protesta masiva sin presencia física.

acciones hacktivistas no buscaban una disrupción a largo plazo del sistema, sino transmitir mensajes en paralelo a los grafitis o bloqueos de protesta fuera de línea.

La segunda fase (2001-2007) comienza con la ruptura geopolítica del 11-S y la consiguiente securitización del ciberespacio. El auge de la Guerra contra el Terror introdujo nuevos marcos legales, programas de vigilancia y límites normativos que criminalizaron cada vez más las actividades hacktivistas. Al mismo tiempo, la proliferación de la banda ancha, así como de la tecnología móvil, facilitó formas de resistencia más sofisticadas. Cabe mencionar que Karatzogianni (2015) distingue dos arquetipos de ciberconflicto durante este período: el etnorreligioso (por ejemplo, las ciberguerras entre India y Pakistán o el conflicto israelí-palestino), y el sociopolítico (por ejemplo, las campañas antiglobalización y contra la guerra). El hacktivismo en esta época se encontraba cada vez más atrapado entre estos polos: desde el *hackeo* patriótico con motivaciones ideológicas hasta las protestas coordinadas contra el Estado. La guerra de Irak de 2003 presenció un auge de la movilización digital, incluyendo campañas masivas de *hackeo* y el uso de blogs para contrarrestar las narrativas mediáticas.

La tercera fase (2007-2010) marcó la emergencia de colectivos hacktivistas como Anonymous y WikiLeaks. Asimismo, las operaciones durante este período combinaron ataques DDoS, filtraciones de información y movilización masiva, que se fusionaron en campañas multiplataforma. Los ataques de 2008 contra la Iglesia de la Cienciología (*Project Chanology*) ejemplificaron esta fase; Anonymous empleó ataques DDoS, protestas reales y medios de comunicación en línea para avergonzar y perturbar a su objetivo. Mientras tanto, la filtración de documentos militares y diplomáticos clasificados por WikiLeaks en 2010 transformó las filtraciones de datos en actos de guerra política, estableciendo con ello un nuevo paradigma para el ciberactivismo como fuerza en las relaciones internacionales.

Como la describe Karatzogianni (2015), la cuarta fase (2010-2014) está marcada por los eventos de la Primavera Árabe (2010-2012)³, los movimientos *Occupy*

³ La Primavera Árabe fue una serie de levantamientos populares ocurridos entre 2010 y 2012 en varios países de Medio Oriente y el Norte de África, incluidos Túnez, Egipto, Libia, Siria, Yemen y Bahrein. Estos movimientos surgieron contra regímenes autoritarios, la corrupción, la pobreza estructural y la represión de las libertades civiles. Lo que caracterizó a estas protestas sociales fue el uso intensivo de redes sociales y plataformas digitales como Facebook, Twitter y YouTube, como instrumentos para organizar protestas, difundir información, documentar abusos y generar presión internacional. Como señala Karatzogianni (2015), la Primavera Árabe demostró el poder simbólico y estratégico del activismo digital, convirtiendo a los ciudadanos en productores de información frente a la censura estatal. Si bien los resultados políticos fueron dispares (desde transiciones frágiles a nuevas formas de autoritarismo), la Primavera Árabe marcó un antes y un después en la historia del ciberactivismo global, al mostrar que las redes digitales podían desempeñar un rol clave en catalizar revoluciones.

(2011-2013)⁴ y las revelaciones de Edward Snowden (2013)⁵. El hacktivismo se vio envuelto en levantamientos democráticos a gran escala, debates sobre vigilancia masiva y luchas globales por la soberanía de la información. En este contexto, el hacktivismo perdió parte de su marginalidad: se incorporó al discurso político dominante, al tiempo que atraía una intensa represión. Tras la Primavera Árabe, la ciberprotesta se celebró como un catalizador democrático, pero también se re-clasificó como una amenaza para la seguridad nacional. Además, la cooptación y criminalización de la protesta digital comenzó a desdibujar las fronteras entre la disidencia y el terrorismo, marcando un punto de inflexión ético crucial.

Partiendo del modelo de cuatro fases de Karatzogianni (2015) sobre hacktivismo y ciberconflicto, una década de desarrollos posteriores obliga a la formulación de al menos dos fases adicionales en la evolución del activismo digital. En opinión del autor de este capítulo, estas fases reflejan no solo los avances técnicos de los últimos años, sino también transformaciones más profundas en la ontología, la función y las implicaciones globales de la resistencia digital. En este sentido, el período comprendido entre 2015 y 2025 ha sido testigo tanto de la intensificación de la guerra cognitiva, de la proliferación de herramientas hacktivistas autónomas y potenciadas por inteligencia artificial (IA), así como del surgimiento de constelaciones de actores híbridos que difuminan los límites entre activismo, guerra y arte de gobernar. Por consiguiente, a continuación se proponen dos nuevas fases en la evolución del hacktivismo:

La quinta fase (2015-2020) estuvo caracterizada por el entrelazamiento geopolítico, la sofisticación táctica y la hibridación del activismo digital con operaciones patrocinadas por el Estado y entidades criminales. Tras las revelaciones

⁴ El movimiento Occupy Wall Street, iniciado en septiembre de 2011 en Nueva York, se expandió rápidamente a decenas de ciudades en todo el mundo bajo la consigna "Somos el 99%", en referencia a la desigualdad económica entre las élites financieras y la ciudadanía general. Occupy se caracterizó por una estructura horizontal y asamblearia, sin líderes definidos, así como por un uso intensivo de herramientas digitales para coordinar acciones, transmitir en vivo (livestreaming) y viralizar mensajes. Occupy demostró cómo las redes sociales podían reemplazar las estructuras organizativas tradicionales y servir como espacio de articulación política (Castells, 2012). Su legado influyó en otras protestas posteriores como "Nuit Debout" en Francia, los "Indignados" en España y el "15-M", y sirvió de antecedente para futuros movimientos como "Black Lives Matter".

⁵ En junio de 2013, Edward Snowden, excontratista de la Agencia de Seguridad Nacional de los Estados Unidos (NSA), filtró a periodistas miles de documentos clasificados que revelaban la existencia de programas masivos de vigilancia global, como PRISM, XKeyscore y Tempora. Estos programas interceptaban llamadas, correos electrónicos, mensajes y metadatos de millones de personas alrededor del mundo, incluso de jefes de Estado aliados. Las filtraciones de Snowden desataron un debate global sobre privacidad, vigilancia estatal y derechos digitales, así como la legitimación de tecnologías de anonimato y cifrado, como Tor, Signal y VPN. Las revelaciones también inspiraron una nueva generación de hacktivistas y defensores de la privacidad digital, reforzando la idea de que el activismo debía enfocarse no solo en lo político, sino también en el control del entorno informacional.

de Snowden y el auge global del ciberescepticismo, el hacktivismo se adentró en un terreno complejo donde la disidencia ideológica se fusionó con la guerra de la información. A diferencia de la cuarta fase, donde la ciberprotesta fue mayoritariamente horizontal y de base, el entorno posterior a 2015 fue testigo de una reutilización estratégica de los métodos hacktivistas tanto por los Estados democráticos como autoritarios.

Campañas de gran repercusión, como la interferencia de Rusia en las elecciones presidenciales estadounidenses de 2016, el uso de herramientas cibernéticas por parte de China en el capitalismo de vigilancia y el autoritarismo digital, y el empleo de cibermilicias por parte de Irán, ilustran la difusa línea que separa el hacktivismo de base de la insurgencia digital impulsada por el Estado (Di Pietro et al., 2021; Kramer et al., 2009). Actores antes etiquetados como “hacktivistas” ahora operan en zonas ambiguas entre la ciberdelincuencia, el ciberespionaje y la guerra ideológica. Por ejemplo, grupos como APT28/Fancy Bear⁶, aunque vinculados a la inteligencia estatal, adoptan con frecuencia la iconografía y la retórica descentralizada del hacktivismo para ocultar sus estructuras de mando. Adicionalmente, el hacktivismo ha madurado tácticamente; los *deepfakes* generados por IA, los mercados de *exploits* de día cero, el *ransomware* como protesta (por ejemplo, NotPetya y WannaCry), y la amplificación sintética de bots han aumentado tanto la escala como la ambigüedad de la disidencia digital (Montasari, 2023). En otras palabras, las herramientas hacktivistas ya no son simplemente disruptivas; ahora se integran en complejas campañas híbridas que afectan las elecciones, los mercados y el derecho internacional.

Sin embargo, esta fase también está marcada por una dilución ideológica. Es decir, la proliferación de actores y la cooptación táctica por parte de las agencias de inteligencia estatales ha erosionado la claridad ideológica del hacktivismo anterior. Por ejemplo, la participación de Anonymous tanto en causas progresistas (#BlackLivesMatter, Operación KKK), como en acciones geopolíticas controvertidas, demuestra el cambiante panorama ético de las operaciones hacktivistas posteriores a 2015 (Karagiannopoulos, 2018).

⁶ “Fancy Bear” y “APT28” son nombres utilizados por expertos en ciberseguridad para referirse a un mismo grupo de amenazas persistentes avanzadas (APT, por sus siglas en inglés: Advanced Persistent Threat), asociado ampliamente con la inteligencia militar rusa, específicamente con la GRU (Dirección Principal del Alto Estado Mayor de las Fuerzas Armadas de Rusia). APT28/Fancy Bear es un grupo de ciberespionaje sofisticado que lleva operando al menos desde 2007, especializado en: 1) ciberataques dirigidos a gobiernos, medios de comunicación, fuerzas armadas, OTAN y ONG; 2) uso de *malware* personalizado, como X-Agent o Sedreco; 3) *spear phishing* avanzado, mediante correos electrónicos con documentos maliciosos adaptados a sus objetivos, y 4) operaciones de exfiltración de datos, sabotaje informativo y campañas de desinformación.

Finalmente, la evolución del hacktivismo se encuentra actualmente en una sexta fase (2020-2025). En efecto, este período se define por tres dinámicas convergentes: 1) el despliegue de agentes digitales autónomos con fines activistas; 2) la integración de las estrategias hacktivistas en la doctrina estatal y la práctica corporativa; y 3) la plataformización de la protesta digital a través de las OAD (organizaciones autónomas descentralizadas) y los colectivos basados en *blockchain*.

En primer lugar, la incorporación de la IA y del aprendizaje automático (*machine learning*) en las herramientas hacktivistas ha transformado la dinámica operativa. Los algoritmos capaces de identificar sistemas vulnerables, diseñar campañas de *phishing* adaptativas o activar fugas de información de forma autónoma, marcan una transición del activismo centrado en el ser humano a la ciberresistencia potenciada por IA. Estos sistemas autónomos plantean nuevos dilemas éticos, a medida que la responsabilidad se distribuye entre actores, algoritmos e infraestructuras (Wilson, 2014).

En segundo lugar, es evidente una creciente institucionalización del hacktivismo en el surgimiento de ONG ciberactivistas, alianzas formales entre tecnólogos disidentes y organizaciones de derechos humanos, e incluso en el establecimiento de programas de *hacking* ético financiados por el Gobierno. La ciberprotesta ya no es un fenómeno externo; está integrada en el discurso público, los marcos regulatorios y las arquitecturas de seguridad corporativa. Los gobiernos ahora practican el hacktivismo sancionado por el Estado bajo doctrinas como ciberdefensa activa y ciberdisuasión, lo que complica aún más la distinción entre protesta y guerra (Koops, 2016).

En tercer lugar, esta fase introduce nuevas formas organizativas. En efecto, las tecnologías *blockchain* han permitido a las OAD orquestrar acciones de protesta, financiar la resistencia civil o ejecutar contratos inteligentes que pueden desencadenar ataques distribuidos cuando se cumplen ciertas condiciones políticas. Por ende, estas protestas programables redefinen la agencia en la contienda digital, ya que la protesta digital se convierte en un evento desencadenado por código y no necesariamente en una decisión humana colectiva. En conjunto, estas dinámicas sugieren que el hacktivismo ya no es meramente reactivo o simbólico, sino que se está convirtiendo en un elemento constitutivo de la actual geopolítica digital, la gobernanza organizacional y la soberanía algorítmica. Es decir, lo que comenzó antes como tácticas de guerrilla en los márgenes de internet ahora resuena en la estrategia ciberdiplomática, los marcos de integridad electoral y los tratados globales de ciberseguridad.

En resumen, la evolución del hacktivismo, desde la disidencia digital simbólica (1994-2001) hasta la agencia infraestructural poshumana (2020-2025), refleja una profunda reconfiguración de la contienda política en la sociedad red (Tabla 1). Las fases quinta y sexta propuestas aquí amplían el modelo de Karatzogianni (2015), al capturar la hibridación, automatización e institucionalización del ciberactivismo en las condiciones de complejidad tecnopolítica y de guerra cognitiva del siglo XXI. Al entrar en una era de maquinaria política autónoma, las implicaciones éticas, legales y estratégicas del hacktivismo exigirán no solo nuevos marcos conceptuales, sino también paradigmas de gobernanza, responsabilidad y derechos en la era digital.

Tabla 1. Seis fases del hacktivismo

Fase	Periodo	Contexto histórico	Actores clave	Tácticas	Enfoque simbólico / estratégico	Tendencias / Resultados
1. Orígenes y disrupción simbólica	1994–2001	Auge de la World Wide Web; zapatismo; protestas antiglobalización	EDT, Culto a la Vaca Muerta, activistas zapatistas en la red	FloodNet, DDoS simbólico, desfiguración de sitios web	Protesta simbólica; desobediencia civil digital	Hacktivismo como representación cultural; surgimiento de la acción directa virtual masiva
2. Auge y polarización Post 11-S	2001–2007	Guerra contra el terrorismo; guerra de Irak; vigilancia global; auge del hacking patriótico	Anonymous (formas iniciales), coaliciones digitales pro/anti-bélicas, grupos de hackers etnonacionalistas	Blogs anti-délicos, robo de sitios web, ciber-guerras (India-Pakistán; Israel-Palestina)	Cuestionamiento de las narrativas estatales; marco antihegemonico	Auge de los conflictos digitales; tensiones étnicas entre activistas y Estados
3. Expansión y disrupción estratégica	2007–2010	Proliferación de la Web 2.0; ciber-conflicto ruso-estonio; crecimiento de redes sociales	Anonymous, LulzSec, Wikileaks	DDoS, filtraciones, ciber-sabotaje, espectáculos mediáticos	Espectáculo político + exposición de datos	Fusión de protesta y performance; aumento de la atención mediática
4. Integración y conflicto de alto riesgo	2010–2014	Primavera Árabe; Occupy Wall Street; revelaciones de Snowden	Colectivos activistas descentralizados, denunciantes, hacktivismo cívico	Transmisiones en directo, cifrado masivo, filtraciones de información, operaciones anónimas	Soberanía de la información; resistencia a la vigilancia masiva	El hacktivismo entra en el discurso político global; legitimación social

Continúa en la otra página

Fase	Periodo	Contexto histórico	Actores clave	Tácticas	Enfoque simbólico / estratégico	Tendencias / Resultados
5. Escalada, híbrida-ción y guerra fría digital	2015–2020	Guerra fría digital; interferencia electoral; ciberpoder global	Hackers estatales (p. ej., Fancy Bear), proxies híbridos, hacktivistas nacionales, hackers éticos politizados	Phishing, botnets, campañas de desinformación, penetración por IA incipiente	Ciberguerra disfrazada de activismo; dilución ideológica	Hacktivismo mezclado con espionaje y cibercriminalidad; instrumentalización estatal
6. Institucionalización y hacktivismo pos-humano	2020–2025	Auge de la IA, activismo blockchain, debates sobre gobernanza de plataformas	OAD, agentes autónomos, ciberONG civiles, hackers éticos	Ataques asistidos por IA, protestas basadas en contratos inteligentes, disidencia generada por código	Protesta programable; ciber-soberanía	Absorción institucional; activismo regido por algoritmos y protocolos; nuevas tensiones Estado-plataforma

Fuente: elaboración propia con base en Karatzogianni (2015).

Tensiones éticas del hacktivismo

Ahora bien, la tensión que define al hacktivismo reside en su ambiguo estatus ético. Para los hacktivistas, es una forma de desobediencia civil, es decir, una respuesta legítima a la injusticia, la censura o el autoritarismo; para los Estados y otras instituciones, a menudo se enmarca como un acto criminal, o incluso terrorista, dependiendo de sus objetivos y sus métodos. Con base en lo anterior, Jordan y Taylor (2004) identifican tres dimensiones interrelacionadas de tensión ética que se encuentran en el núcleo de la práctica hacktivista: el conflicto entre medios y fines, el riesgo de daño público versus privado, y el problema de la rendición de cuentas en acciones descentralizadas y anónimas. Estas tensiones siguen siendo fundamentales para evaluar la legitimidad y las consecuencias del ciberactivismo tanto en contextos democráticos como autoritarios.

Uno de los debates éticos más importantes en el hacktivismo es si la ilegalidad de los medios se justifica por la rectitud de los fines. Las tácticas hacktivistas (como las intrusiones no autorizadas, los ataques DDoS y la filtración de datos clasificados), a menudo violan las leyes nacionales y las normas de ciberseguridad. Sin embargo, los hacktivistas suelen defender que estos métodos son necesarios para exponer la corrupción, resistir el autoritarismo o proteger los derechos humanos.

Por ejemplo, la desfiguración de sitios web gubernamentales durante la Primavera Árabe o los ataques DDoS de Anonymous en respuesta a la persecución

de WikiLeaks fueron vistos por sus simpatizantes como desobediencia civil digital: intervenciones no violentas, pero técnicamente ilegales, destinadas a defender la libertad de información o apoyar la movilización política (Coleman, 2014). El dilema, como señalan Jordan y Taylor (2004), radica en si violar la legislación informática es éticamente defendible cuando sirve a una causa alineada con los valores democráticos. Esta tensión refleja debates anteriores en filosofía política, como la justificabilidad de la desobediencia civil o el sabotaje en contextos represivos. La pregunta sigue vigente: ¿mitiga la intención emancipadora del hacktivismo la ilegalidad de sus métodos, o deberían las normas legales permanecer inviolables independientemente de la motivación?

La segunda dimensión aborda las consecuencias imprevistas de las acciones hacktivistas. Aunque la mayoría de las campañas se dirigen a instituciones poderosas (gobiernos, corporaciones multinacionales, contratistas de vigilancia), sus tácticas pueden perjudicar inadvertidamente servicios públicos o a particulares. Por ejemplo, un ataque DDoS contra un ministerio puede interrumpir el acceso a servicios públicos vitales como la declaración de impuestos, los sistemas de inmigración o las plataformas de datos sanitarios. De igual manera, la exposición de documentos o filtraciones de datos, al tiempo que se atacan irregularidades institucionales, puede revelar inadvertidamente información personal de empleados, terceros o denunciantes, violando su privacidad o poniendo en peligro su seguridad.

Sauter (2014) argumenta que los ataques DDoS, como los desplegados en la Operación Venganza⁷, pueden considerarse como “bloqueos simbólicos” similares a las protestas callejeras. Sin embargo, si bien las sentadas físicas suelen estar contenidas espacial y temporalmente, la naturaleza interconectada de la infraestructura digital implica que las interrupciones pueden propagarse a través de los sistemas, amplificando los daños no deseados (Drmola et al., 2015). Por lo tanto, los hacktivistas deben sopesar la legitimidad moral de su objetivo frente a los daños colaterales que podrían infligir a los no combatientes.

El tercer dilema ético surge de la naturaleza descentralizada y anónima de la mayoría de los colectivos hacktivistas existentes. Movimientos como Anonymous evitan deliberadamente las estructuras jerárquicas o un liderazgo identificable,

⁷ “Operation Payback” fue una campaña de ciberprotesta impulsada por Anonymous entre 2010 y 2011, que empleó ataques DDoS contra corporaciones como Visa, PayPal y Mastercard, primero en defensa del intercambio de archivos y luego como respuesta al bloqueo financiero impuesto a WikiLeaks. Considerada un caso paradigmático del hacktivismo postmoderno, esta operación ejemplifica el uso táctico de interrupción digital como forma de resistencia simbólica frente al poder corporativo y estatal.

adoptando una lógica de “somos legión”. Si bien esta descentralización fomenta la inclusión y la resiliencia frente a la represión, también dificulta la responsabilidad moral y legal. Cuando las operaciones hacktivistas resultan en daños desproporcionados, sabotaje interno o violaciones legales, no existe un mecanismo claro de responsabilidad. Como se cuestionan Jordan y Taylor (2004), cuando “todos somos Anonymous”, ¿quién asume la responsabilidad de los daños colaterales, los errores de cálculo estratégico o las violaciones éticas?

Coleman (2014) explora cómo la gobernanza interna dentro de Anonymous se negocia informalmente a través de foros de chat, memes y dinámicas de reputación. Sin embargo, estos mecanismos son volátiles y fácilmente manipulables. La ausencia de transparencia o protocolos de consenso dificulta garantizar que las operaciones estén éticamente alineadas o incluso sean respaldadas colectivamente. Esto plantea serios desafíos para la legitimidad; a diferencia del activismo convencional (donde líderes, ONG u organizadores pueden rendir cuentas por los resultados), el hacktivismo opera en un espacio donde la gobernanza ética es *a posteriori*, reactiva y, a menudo, ambigua.

Las tensiones éticas descritas por Jordan y Taylor (2004) resaltan la complejidad normativa de la resistencia digital. En consecuencia y a medida que el hacktivismo evoluciona en alcance, tecnología e impacto, estos dilemas se acentuarán. Esto invita al cuestionamiento crítico no solo de la moralidad de las acciones individuales, sino también de los marcos más amplios mediante los cuales se conceptualiza, legitima y cuestiona la protesta digital en un orden de información globalizado. Uno de los debates éticos más polémicos gira en torno a los ataques DDoS. Sus defensores argumentan que son similares a las sentadas digitales: interrupciones no violentas y simbólicas del poder. Los críticos argumentan que socavan la libertad de expresión y el acceso, creando un efecto disuasorio (Sauter, 2014). De igual manera, las filtraciones de datos plantean cuestiones de privacidad frente a interés público. Las revelaciones de WikiLeaks en 2010 desencadenaron un debate global: ¿tienen los ciudadanos derecho a saber qué hacen los Estados en su nombre?; ¿o ponen estas filtraciones en peligro vidas y la diplomacia?

En conclusión, el hacktivismo es una expresión paradigmática de la contienda política en la era digital. Su historia, trazada a través de las seis fases del activismo digital, revela una trayectoria que va desde la disrupción simbólica hasta la agencia poshumana. Ha desafiado no solamente las estructuras de poder, sino también los marcos éticos tradicionales en torno a la protesta, la rendición de cuentas y la resistencia. A medida que las infraestructuras digitales se integran

más profundamente en la gobernanza y la sociedad, los riesgos del hacktivismo seguirán aumentando. La ambigüedad de su estatus (como protesta, delito o guerra) exige no solo una mejor regulación, sino también una reflexión ética más matizada. Lo que queda claro es que el hacktivismo no es una tendencia transitoria ni una amenaza externa; es una expresión en evolución de la agencia política digital que dará forma al futuro del disenso.

Impulsores del hacktivismo

La evolución del hacktivismo, como forma distintiva de acción política, también se basa en una confluencia de marcos ideológicos que buscan responder a las cambiantes arquitecturas de poder, control y vigilancia en la era digital. Si bien el hacktivismo carece de un único núcleo doctrinal, se articula consistentemente en torno a tres impulsores ideológicos: libertarismo digital, anticorporativismo y activismo antivigilancia. Estas tres corrientes convergen en la defensa de internet como un dominio libre, descentralizado y autónomo, que resiste las intrusiones tanto de la soberanía estatal como de la hegemonía corporativa. La interacción entre estas ideologías produce una forma dinámica de ciberresistencia que es a la vez moral, política y técnica.

Libertarismo digital: autonomía, acceso y libertad algorítmica

El libertarismo digital es quizás el impulso ideológico más antiguo y fundamental del hacktivismo. Surgido de la ética *hacker* de las décadas de 1960 y 1970, y adquiriendo mayor claridad filosófica en la década de 1990, este imaginario concibe internet como un espacio radicalmente descentralizado de autonomía personal y autogobierno, libre de la supervisión coercitiva estatal o corporativa. Su linaje intelectual se remonta a figuras como John Perry Barlow, Timothy Leary y Eric S. Raymond, así como a las corrientes libertarias de la literatura ciberpunk y el movimiento del código abierto.

La influyente obra de Barlow (1996) captura esta visión sucintamente, afirmando que los gobiernos “no tienen soberanía donde nos reunimos”. Este imaginario libertario concibe el ciberespacio no solo como un medio de comunicación, sino como un espacio jurídico y ontológico distinto del mundo analógico: un ágora digital donde la libertad, y no la ley, es el principio rector. Raymond (2001) articula de manera similar una visión de sistemas de conocimiento ascendentes, producidos por pares, que resisten el control jerárquico y los modelos de producción centralizados.

Por consiguiente, el hacktivismo, inspirado en el libertarismo digital, suele atacar la censura en internet, los cortafuegos estatales y los marcos regulatorios considerados incompatibles con la autonomía digital. Por ejemplo, el apoyo hacktivista al Proyecto Tor, I2P y las redes VPN representa una respuesta técnica a los intentos de los regímenes autoritarios de controlar los flujos de información digital (Karatzogianni, 2015). Campañas como #OpTunisia durante la Primavera Árabe u #Oplran tras la represión electoral ejemplifican el despliegue táctico de herramientas de cifrado, sitios espejo y redistribución de información para subvertir la censura. Esta ideología también fundamenta la ética *hacker* de que la información debe ser libre, lo que ha motivado numerosas campañas para publicar información clasificada o privada; desde WikiLeaks hasta plataformas descentralizadas de denuncia como GlobaLeaks, estos proyectos articulan una visión de transparencia radical como freno al poder, una lógica que a menudo entra a cuestionar la legitimidad de la propia propiedad intelectual.

Sin embargo, el libertarismo digital no está exento de contradicciones internas. Su énfasis retórico en la libertad individual puede colisionar con los objetivos colectivos, especialmente en redes de resistencia global que deben negociar la diversidad cultural y política. Además, su desconfianza hacia las instituciones puede generar reticencia a participar en la construcción de alianzas estratégicas, lo que limita su capacidad para generar cambios sistémicos (Jordan & Taylor, 2004).

Anticorporativismo: resistencia al capitalismo de vigilancia y al cercamiento digital

La segunda gran corriente ideológica del hacktivismo es el anticorporativismo, que surge en respuesta a la creciente consolidación de la infraestructura digital y los flujos de información bajo el control de corporaciones tecnológicas transnacionales. Mientras que los libertarios digitales se resisten al control estatal, los anticorporativistas se resisten principalmente a la mercantilización de la información y al cercamiento de los bienes comunes digitales por parte de actores privados. Esta crítica se alinea con movimientos antineoliberales más amplios que cuestionan la desregulación de los mercados, la privatización de los servicios públicos y el poder político del capital multinacional. En el ámbito digital, se centra en lo que Zuboff (2019) denomina capitalismo de vigilancia, es decir, la monetización del comportamiento del usuario mediante análisis predictivos y manipulación del comportamiento. Por lo tanto, las acciones hacktivistas en este contexto buscan exponer las prácticas de explotación de datos de gigantes tecnológicos como Google, Facebook, Amazon y Microsoft.

Históricamente, esta postura ideológica se ejemplificó con la Operación Venganza (2010), en la que Anonymous realizó ataques DDoS contra PayPal, Visa y Mastercard en represalia por su bloqueo financiero a WikiLeaks (Coleman, 2014). Estas acciones no solo apoyaban a Assange o la libertad de expresión; eran confrontaciones simbólicas con la complicidad corporativa en la censura estatal. De igual manera, los ataques contra asociaciones de la industria del entretenimiento como la RIAA y la MPAA cuestionaron la monopolización de la cultura y la criminalización del intercambio de archivos. Burnett y Vescina (2017) enmarcan el hacktivismo de este modo como una respuesta a la vigilancia y la mercantilización corporativas, donde los individuos se convierten en conjuntos de datos ambulantes, comercializados dentro de mecanismos opacos del mercado. En consecuencia, el hacktivismo anticorporativo cuestiona tanto la ética de estas economías como las arquitecturas legales privatizadas (por ejemplo, los regímenes de eliminación de la DMCA) que las sustentan.

Además, los hacktivistas han intervenido repetidamente en momentos de protesta global contra las instituciones neoliberales. Durante las protestas de *Occupy Wall Street* de 2011, Anonymous lanzó #OpWallStreet, filtrando información de empresas financieras y publicando imágenes de brutalidad policial. Asimismo, en América Latina, los colectivos hacktivistas han atacado a corporaciones extractivistas involucradas en la degradación ambiental y el desplazamiento de comunidades indígenas (Guarín, 2023). Finalmente, el anticorporativismo a menudo opera en alianza táctica con el libertarismo digital, pero su énfasis ideológico es más materialista y estructural, considerando internet no solo como un espacio de expresión, sino como un campo de batalla de explotación económica y resistencia.

Antivigilancia: disidencia digital en la era de la recopilación masiva de datos

El tercer motor ideológico central es el activismo antivigilancia, que ha cobrado cada vez mayor relevancia en la era posterior a Snowden. Las revelaciones de Edward Snowden en 2013 sobre el programa PRISM de la NSA y su colaboración con empresas tecnológicas para llevar a cabo vigilancia global transformaron radicalmente el panorama discursivo de la política digital. La exposición de la recopilación masiva de datos por parte de las agencias de inteligencia estatales (incluidas la NSA, el GCHQ y sus aliados de los "Cinco Ojos") impulsó una ola de acciones hacktivistas basadas en la defensa de la privacidad, las libertades civiles y la autonomía informativa.

Desde entonces, grupos hacktivistas como Anonymous, LulzSec y AntiSec han intensificado su enfoque en los aparatos de vigilancia estatales y sus socios del sector privado. Por ejemplo, el ataque informático a HBGary Federal en 2011 fue una represalia directa por el papel de la empresa en el desarrollo de herramientas de vigilancia y el intento de infiltrarse en Anonymous. La filtración resultó en la publicación de más de 60 000 correos electrónicos internos, exponiendo una trama entre los contratistas de ciberseguridad y agencias de inteligencia estadounidenses (Karagiannopoulos, 2018). Pero el activismo antivigilancia no se limita a las democracias liberales occidentales. En China, Irán, Rusia y otros contextos autoritarios, grupos hacktivistas, tanto internos como en el extranjero, han desarrollado herramientas para eludir los cortafuegos, ocultar identidades y exponer la propaganda estatal. El caso de las protestas prodemocráticas de Hong Kong en 2019 ilustra cómo la ideología antivigilancia configura la resistencia: los activistas desarrollaron aplicaciones de mapeo en tiempo real para evadir a la policía, utilizaron mensajería cifrada como Signal y emplearon punteros láser para desactivar los sistemas de reconocimiento facial.

Filosóficamente, el activismo antivigilancia se ha nutrido de las tradiciones de autodeterminación informativa y resistencia en red a regímenes panópticos. Es decir, considera los datos no como un recurso neutral, sino como un vector de poder, donde su recopilación, almacenamiento y análisis estructuran el comportamiento de individuos y poblaciones. En este marco, incluso la acumulación de datos "inofensiva" se convierte en un espacio de lucha, ya que reconfigura lo que Foucault (1977) describió en su momento como las tecnologías del yo. Es importante destacar que el activismo antivigilancia también se vincula con movimientos más amplios por la justicia racial, la igualdad de género y los derechos de los refugiados, que reconocen cada vez más que la vigilancia digital exacerba las formas existentes de discriminación y control. Los algoritmos de vigilancia predictiva, las tecnologías de monitoreo fronterizo y los sistemas de rastreo biométrico afectan de manera desproporcionada a los grupos marginados, ampliando así el alcance de la resistencia hacktivista para abarcar luchas interseccionales.

Si bien el libertarismo digital, el anticorporativismo y el activismo antivigilancia son analíticamente distintos, en la práctica se superponen y se refuerzan mutuamente, formando una constelación de resistencia contra diferentes modalidades de dominación digital. El hacktivismo se convierte así en una formación híbrida, ni puramente ideológica ni puramente táctica, sino moldeada por diversas redes, contextos y actores.

No obstante, persisten las contradicciones; por ejemplo, el escepticismo de los libertarios digitales ante la intervención estatal puede, en ocasiones, coincidir incómodamente con sentimientos antirregulatorios que también favorecen los intereses corporativos. Las estrategias anticorporativistas que dependen de la filtración de información sensible pueden entrar en conflicto con los principios de privacidad. Y las campañas antivigilancia que valoran el anonimato y el cifrado pueden tener dificultades para escalar o construir instituciones duraderas.

Por lo tanto, el hacktivismo se entiende mejor no como un movimiento unificado, sino como un campo de disputa política, donde ideologías superpuestas se enfrentan a enemigos comunes mediante formas asimétricas, descentralizadas y, a menudo, simbólicas de insurgencia digital. En consecuencia, su poder reside en su capacidad de adaptación para mutar en respuesta a amenazas emergentes, ya sean de Estados, mercados o sistemas de gobernanza algorítmica.

Políticas de identidad posmodernas, protesta en red y resistencia simbólica

El hacktivismo está profundamente arraigado en el panorama sociocultural de la posmodernidad, marcado por la descentralización, la performatividad y la confrontación simbólica, más que por demandas ideológicas coherentes. A diferencia del activismo tradicional impulsado por afiliaciones institucionales o ideologías políticas de masas, el hacktivismo opera mediante una mezcla de memes, máscaras, estética y anonimato. Su surgimiento señala una transformación más amplia en el compromiso político, en la que la identidad, la estructura en red y la subversión semiótica sustituyen a los manifiestos programáticos.

Como argumenta Karatzogianni (2015), el hacktivismo ejemplifica una forma de ciberguerra impulsada por la resistencia ideológica, cultural y simbólica, más que por objetivos geopolíticos. Esta transformación, enmarcada en las condiciones de la posmodernidad, difumina las fronteras entre *performance* y protesta, sátira y sabotaje, espectáculo y estrategia. A diferencia de las lógicas políticas modernistas basadas en el discurso racional y el liderazgo jerárquico, el hacktivismo posmoderno prospera gracias a la fragmentación, la ironía transgresora y la circulación viral, obteniendo su poder no de la legitimidad institucional, sino de la resonancia cultural y la disrupción simbólica.

La posmodernidad, tal como la articulan teóricos como Lyotard (1984) y Baudrillard (1994), rechaza las grandes narrativas y prioriza las identidades fragmentadas, las simulaciones y los signos culturales. El hacktivismo se integra en

este cambio epistémico; como señalan Jordan y Taylor (2004), el hacktivismo no exige la coherencia total del activismo tradicional; se vale del *performance*, la parodia y la polifonía. Esto se ejemplifica en la estética y el simbolismo de la máscara de Guy Fawkes (popularizada por *V de Vendetta*), el uso de la cultura de los memes en internet y la apropiación de símbolos corporativos y gubernamentales en campañas de desfiguración digital. Estas no son características accidentales, sino intervenciones deliberadas en la política de la representación, diseñadas para socavar, ridiculizar o invertir los significados dominantes.

La cultura del lulz⁸ asociada a Anonymous, como documentan Sauter (2014) y Coleman (2014), encarna esta lógica simbólica, en donde las acciones no son tan solo políticas, sino también cómicas, absurdas y carnales; efectivamente, esta fusión de diversión y agresión conforma un modo de interacción posideológico, donde, por ejemplo, la política está mediada por la ironía, el troleo y el espectáculo. Por ende, el hacktivismo no es solo un acto tecnológico; también se constituye como un evento discursivo. En otras palabras, las acciones hacktivistas no son meramente destructivas, sino intervenciones semióticas destinadas a desestabilizar la autoridad narrativa de sus objetivos; esto incluye la filtración de documentos sensibles, la desfiguración de sitios web estatales con memes políticos o la creación de un revuelo en redes sociales con campañas de hashtags, como aquella viralizada durante el “estallido social” en Colombia en 2019 y 2021, mediante la campaña #NosEstanMatando.

La estructura de los movimientos hacktivistas refleja el análisis de Castells (2012) sobre los movimientos sociales en red: horizontales, descentralizados y fluidos. Como afirman Karagiannopoulos (2018) y Milan (2015), las redes hacktivistas como Anonymous no son organizaciones jerárquicas, sino conjuntos de actores con afiliaciones flexibles que se unen temporalmente en torno a causas o símbolos compartidos. La metáfora del rizoma⁹, desarrollada por Deleuze y

⁸ La “cultura del lulz”, derivada de la jerga de Internet “lol” (*laugh out loud*), hace referencia a una forma de acción digital basada en la burla, el troleo y el placer de subvertir normas sociales o institucionales. En el contexto del hacktivismo, especialmente en colectivos como Anonymous o LulzSec, el “lulz” representa una motivación ambigua que combina humor transgresor con crítica política. Más que buscar reformas explícitas, muchas de sus acciones se diseñan para exponer contradicciones, ridiculizar al poder o generar caos simbólico.

⁹ Deleuze y Guattari (1987) utilizan el rizoma como metáfora para desafiar los modelos occidentales tradicionales de conocimiento y organización social, que suelen ser arborescentes, es decir, con forma de árbol, estructurados jerárquicamente a partir de una raíz u origen (como Dios, el Estado o el sujeto soberano). En contraste, el rizoma representa: 1) multiplicidad en lugar de unidad; 2) conectividad y heterogeneidad (cualquier punto puede conectarse con cualquier otro); 3) descentralización (sin autoridad central ni origen); 4) aciclicidad (sin principio ni fin, solo intermedios); y 5) ensamblajes que pueden desmantelarse y reensamblarse dinámicamente. Por lo tanto, el hacktivismo es rizomático: no es un movimiento singular con una

Guattari (1987), describe sistemas no jerárquicos, descentralizados y no lineales; en el contexto del hacktivismo, esta metáfora permite comprender cómo colectivos como Anonymous operan de forma distribuida, sin líderes definidos ni estructuras fijas, adaptándose continuamente mediante redes horizontales digitales.

Así, el hacktivismo contemporáneo encarna una lógica rizomática, en donde las redes hacktivistas crecen en direcciones impredecibles, sin raíces centralizadas ni un liderazgo claro. Cabe señalar que esto no es una debilidad, sino una ventaja estratégica, que facilita la agilidad, la redundancia y la opacidad. Romagna y Leukfeldt (2024a) demuestran que las redes hacktivistas operan en un espectro de organización, desde colaboraciones *ad hoc* entre pares hasta equipos extensos con roles definidos y códigos de conducta internos.

Plataformas digitales como IRC, Telegram y la *dark web* funcionan como entornos de convergencia donde los hacktivistas coordinan acciones, comparten herramientas y realizan rituales de identidad colectiva (Leukfeldt y Holt, 2020). Este tipo de plataformas permiten una coordinación rápida sin copresencia física y fomentan lo que Milan (2015) denomina individualismo en red, una forma de pertenencia basada en vínculos flexibles y afectivos, en lugar de una membresía organizacional duradera. Esta dinámica se hizo evidente en #OpTunisia (2011), donde Anonymous y otros utilizaron canales de IRC para coordinar el apoyo a los manifestantes durante la Primavera Árabe. La operación incluyó ataques DDoS, sitios espejo digitales y la difusión de herramientas anticensura. Asimismo, ningún actor en particular lideró la operación; más bien, surgió a través de comportamientos de enjambre, el uso de memes y la difusión de una narrativa compartida de solidaridad antiautoritaria (Karatzogianni, 2015).

El hacktivismo prospera no solo a través del código, sino también a través de la teatralidad. Lo que Jordan (2002) denominó sabotaje semiótico sigue siendo un arma vital, es decir, la apropiación, la desfiguración o la suplantación de símbolos digitales para exponer las contradicciones del poder. Estas acciones operan en la tradición del *jamming* cultural (Lasn, 1999), desafiando los significados dominantes mediante el *détournement* y la sátira. Por ejemplo, la Operación Venganza se dirigió a medios de comunicación y corporaciones financieras consideradas cómplices de la censura, en particular por su retirada de los servicios de WikiLeaks. Pero el espectáculo de la operación (sus memes, manifiestos y videos de YouTube) fue tan significativo como su impacto técnico. La acción se convirtió

doctrina unificada, sino una multiplicidad de resistencias, identidades y discursos locales que se cohesionan temporalmente a través de memes compartidos, indignación moral o blancos digitales.

en un acontecimiento mediático, aprovechando la lógica de la viralidad para amplificar su mensaje político (Sauter, 2014; Coleman, 2014).

LulzSec, una escisión de Anonymous¹⁰, encarnó esta lógica performativa de forma aún más radical. En 2011, hackeó el sitio web de la Agencia Central de Inteligencia (CIA), la *PlayStation Network* de Sony y *Fox News* no solo para exponer vulnerabilidades, sino también para burlarse del espectáculo de la seguridad estatal y corporativa; sus comunicados a menudo mezclaban sátira y seriedad, exponiendo cómo el humor se convierte en una forma de crítica y resistencia. Estas tácticas concuerdan con la noción de hiperrealidad de Baudrillard (1994), donde las simulaciones y representaciones se vuelven más poderosas que la realidad misma. El hacktivismo interviene en la economía simbólica de los signos, no solo en la infraestructura; como tal, es al mismo tiempo un ataque a los sistemas como una deconstrucción de las narrativas que los legitiman.

El conflicto entre Rusia y Ucrania ilustra la transformación del hacktivismo en un componente de guerra híbrida. Desde 2014, los grupos hacktivistas han atacado tanto a actores estatales como no estatales, combinando activismo, patriotismo y lógica paramilitar. En 2022, Anonymous lanzó #OpRussia, atacando sitios web del Kremlin y medios de comunicación estatales en represalia por la invasión. Esto fue reflejado por grupos prorrusos como KillNet, que atacaron activos ucranianos, de la Unión Europea (UE) y de la Organización del Tratado del Atlántico Norte (OTAN).

Por su parte, el surgimiento del Ejército Informático de Ucrania, una milicia digital descentralizada, ejemplifica el hacktivismo sancionado por el Estado, coordinado a través de plataformas como Telegram y compuesto tanto por ciudadanos ucranianos como por voluntarios extranjeros; como documentan Romagna y

¹⁰ "Anonymous", el icónico colectivo hacktivista, surgió del foro /b/ de 4chan, un espacio de anarquismo digital donde el troleo y la irreverencia coexistían con la indignación moral. Como documenta Coleman (2014), Anonymous evolucionó del juego caótico al compromiso político, especialmente durante el Proyecto Chano-logy, una campaña contra la Cienciología. Esta operación incluyó ataques DDoS, spam telefónico y protestas físicas: un ejemplo de protesta híbrida entre lo digital y lo corpóreo. Acciones posteriores, como la Operación Payback (dirigida a Visa y PayPal tras el bloqueo financiero de WikiLeaks) y #OpISIS, revelaron la transformación de Anonymous en un enjambre glocal: con raíces locales pero movilización global (Karatzogianni, 2015; Sauter, 2014). Estas operaciones difuminaron las fronteras entre espectáculo y sabotaje, protesta y broma. "LulzSec", en cambio, surgió como un subgrupo explícitamente performativo, orientado al humor, la transgresión y la visibilidad. Sus ataques contra la CIA y Sony no exigieron reformas políticas, sino que expusieron la inseguridad institucional. Según Karagiannopoulos (2018), las acciones de LulzSec se situaron en un espacio entre la rebelión carnavalesca y el terrorismo digital, enfatizando el poder ambivalente de la risa como arma política. Su caída, precipitada por los arrestos de 2011-2012, ilustra la tensión entre la identidad colectiva fluida y la represión estatal, revelando cómo las libertades anárquicas de la protesta en red son vulnerables a la infiltración y la cooptación.

Leukfeldt (2024a), estas redes muestran características de una organización compleja, con roles definidos, reglas de coordinación y resiliencia operativa. La guerra ruso-ucraniana ha puesto de relieve una profunda difuminación entre actores estatales, civiles y criminales, donde la desfiguración simbólica, las filtraciones de datos y las campañas DDoS son tan importantes como la acción militar cinética. En este caso, el hacktivismo no es meramente performativo, sino estratégico e instrumental, integrado en cálculos geopolíticos más amplios.

Con base en lo anterior, el hacktivismo en la era posmoderna no puede entenderse únicamente desde la perspectiva del activismo tradicional. Debe interpretarse como una guerra simbólica, representada mediante memes, performatividad y la lógica viral de la protesta en red. La convergencia de la política identitaria, la coordinación distribuida y la resistencia semiótica redefine tanto los medios como los fines de la acción política. Ya sea lanzando ciberataques en zonas de guerra, desfigurando sitios web corporativos para protestas ideológicas o realizando *performances* virales para desafiar los regímenes de vigilancia, los hacktivistas aprovechan las posibilidades culturales y comunicativas de la era digital. Su poder reside no solo en alterar la infraestructura, sino también en alterar el significado; es decir, en librar una guerra no solo contra los sistemas, sino también contra los símbolos que los sustentan.

Movimientos de protesta digital en América Latina

El hacktivismo abarca un espectro de actividades digitales disruptivas motivadas por agendas sociopolíticas (Jordan & Taylor, 2004). Dentro de este espectro se encuentra una variante particular conocida como hacktivismo performativo, el cual hace referencia a los actos expresivos de resistencia en línea que están impulsados ideológicamente, y en donde se priorizan la visibilidad simbólica y la provocación retórica sobre la disrupción operativa (Workman et al., 2013). A diferencia de los ciberataques encubiertos dirigidos a la infraestructura, el hacktivismo performativo se nutre del espectáculo, la intensidad comunicativa y la dinámica subcultural de la protesta digital. Paralelamente, la estructura y evolución de redes hacktivistas exigen una atención minuciosa a cómo interactúan los vínculos sociales en línea y fuera de línea para crear comunidades de resistencia; parece ser que estas redes no surgen simplemente de encuentros digitales aislados, sino, por el contrario, de complejos procesos de oportunidad social y entornos de convergencia, así como de afinidad ideológica. El estudio de Romagna y Leukfeldt (2024b) sobre las redes hacktivistas revela que los entornos en línea, más que los vínculos fuera de línea,

son los principales impulsores del reclutamiento, la socialización y la coordinación operativa.

Por su lado, Workman et al. (2013) definen el hacktivismo performativo como una práctica subcultural distintiva, en donde la disidencia política se manifiesta mediante la retórica abusiva, el sabotaje reputacional y los intentos de dominar el discurso en línea. Se diferencia del *cracking* político tradicional (por ejemplo, desfiguración de sitios web), por su carácter simbólico y retórico; por lo tanto, los hacktivistas performativos hacen uso de la visibilidad de las plataformas como arma para ridiculizar, avergonzar o deslegitimar a su objetivo, a menudo invocando diferentes herramientas de disidencia, como la sátira, la ironía o la indignación moral.

Según Workman et al. (2013), estos comportamientos se basan en la intensidad afectiva, el compromiso ideológico y el refuerzo subcultural. Basándose en teorías de la acción colectiva, así como del contagio social, Workman et al. (2013) conceptualizan las subculturas hacktivistas performativas como comunidades emergentes moldeadas por guiones emocionales compartidos, agravios políticos y viralidad digital. Los grupos se forman en torno a la afinidad de ideas, donde el refuerzo mutuo crea cámaras de resonancia de la disidencia. Las normas dentro de estos grupos a menudo se desvían de las expectativas sociales, mostrando tolerancia (o incluso fomento), del discurso virulento y antagónico bajo la apariencia de resistencia moral.

Crucialmente, el hacktivismo performativo también está codificado culturalmente. Se basa en gran medida en memes, lenguaje simbólico e imágenes contraculturales. Marcadores estéticos como las máscaras de Guy Fawkes o los hashtags con eslóganes se utilizan para producir resistencia semiótica, un tipo de protesta que no se libra mediante armas ni votos, sino mediante símbolos y visibilidad (Karatzogianni, 2015; Coleman, 2014). Además, la formación de la identidad hacktivista en las subculturas performativas está estrechamente vinculada a la pertenencia afectiva, la desindividuación y la creación de narrativas colectivas. Como teorizan teóricos de la identidad social como Tajfel y Turner (1979), los participantes del hacktivismo performativo se validan no solo por sus acciones, sino también por pertenecer a un endogrupo que comparte posturas adversarias hacia las instituciones hegemónicas.

En grupos que exhiben alta intensidad afectiva, los individuos suelen suspender su autonomía crítica y seguir las normas del grupo incluso cuando se apartan de los límites éticos personales; esta desindividuación contribuye a la escalada de la violencia retórica y justifica acciones no normativas como la burla, el desprecio

o el acoso selectivo, en lo que Workman et al. (2013) han venido en denominar ciclos de escalada emocional. Estas subculturas también exhiben jerarquías internas enmascaradas por afirmaciones de descentralización; si bien el anonimato es un principio fundamental, los sistemas de reconocimiento performativo (a través de etiquetas, seudónimos o credibilidad digital) crean economías de prestigio dentro de las redes. Esto contribuye a la cohesión interna, pero también a la competencia intrasubcultural, ya que los miembros se esfuerzan por superarse unos a otros en audacia retórica o sabotaje digital.

En las últimas décadas, América Latina se ha convertido en un territorio vibrante y complejo para la articulación del hacktivismo, en varias de sus modalidades, incluyendo el performativo, ya que la convergencia de antiguas tradiciones de movilización popular con nuevas posibilidades tecnológicas ha generado modalidades distintivas de política contenciosa. En efecto, desde las calles de Caracas o Santiago de Chile hasta las redes en Tegucigalpa, desde la radio comunitaria en Chiapas hasta las campañas de TikTok en Bogotá D.C., los medios digitales han propiciado una transformación en la forma en que se expresa, se media y se impugna la disidencia. Empero, esta transformación no es lineal ni es uniformemente progresiva, ya que su desarrollo se lleva a cabo en contextos de persistentes desigualdades e inestabilidad sociopolítica, revelando la ambivalencia de las tecnologías digitales como herramientas de emancipación e instrumentos de control.

El hacktivismo latinoamericano se mueve entre tres paradigmas interpretativos. El primero, el ciberoptimismo, considera las plataformas digitales como facilitadoras de la democratización y la participación horizontal. El segundo, el ciberpesimismo, se centra en la vigilancia digital, la desinformación y la mercantilización de la disidencia. El tercero, más integrador, entiende la protesta digital como un ensamblaje sociotécnico moldeado tanto por las prácticas de los usuarios y las condiciones infraestructurales, así como por los contextos políticos. Tal como señala Olmedo (2022), estas perspectivas mencionadas no son mutuamente excluyentes; se superponen y se cruzan en la praxis de los activistas digitales de toda la región.

En este contexto, el paro nacional de 2021 en Colombia ofrece un caso de estudio vívido. Inicialmente desencadenado por una reforma tributaria propuesta por el gobierno, el paro evolucionó rápidamente a un levantamiento multisectorial y multigeneracional que expresó reclamos más profundos relacionados con la desigualdad socioeconómica, el desempleo juvenil, la violencia policial y la desconfianza institucional. Sin embargo, lo que realmente distinguió a las protestas

de 2021 fue el grado en que las plataformas digitales (Twitter, Instagram, TikTok, WhatsApp), se convirtieron en un elemento central para su organización, difusión y fuerza afectiva.

El hacktivismo en Colombia durante este período se configuró como un ecosistema híbrido, donde las acciones en línea y fuera de línea se complementaban. Etiquetas como #ParoNacional, #SOSColombia y #NosEstanMatando fueron tendencia global, llamando la atención sobre la presunta represión estatal y movilizand la solidaridad internacional. Al mismo tiempo, las protestas físicas se transmitieron en vivo a través de redes sociales, y aparentes casos de brutalidad policial se documentaron en tiempo real, desafiando las narrativas oficiales y amplificand las voces de las bases¹¹. Esta dinámica ilustra lo que los académicos llaman acción conectiva, un modo de protesta que se basa en contenido personalizado y digitalizado en lugar de estructuras organizativas formales.

La dimensión afectiva de las protestas fue particularmente relevante. Videos de TikTok de manifestantes bailando en las calles, testimonios de ciudadanos heridos o en duelo, y expresiones artísticas virales crearon comunidades emocionales basadas en la indignación, la esperanza y la solidaridad. En otras palabras, no se trataba simplemente de productos informativos; eran representaciones afectivas que ayudaron a construir la identidad colectiva y a movilizar la participación. Según Téllez (2023), plataformas como El Avispero funcionaron como comunidades de sentimiento, traduciendo la resonancia emocional en compromiso político.

Empero, las capacidades expresivas de las herramientas digitales coexistieron con importantes limitaciones estructurales. El acceso a internet siguió siendo profundamente desigual. Para el 2021, casi la mitad de la población del país carecía de acceso constante a internet, una situación que se agravó en las zonas rurales y urbanas marginadas. Esta brecha digital significó que, si bien algunas comunidades pudieron participar plenamente en la protesta digital, otras permanecieron excluidas o dependientes de intermediarios. A pesar de estas limitaciones, la dimensión digital de la protesta de 2021 amplió el alcance espacial y temporal, ya que algunos colombianos residentes en el exterior, especialmente en Europa,

¹¹ Si bien la circulación de videos en redes sociales permitió visibilizar presuntos casos de abuso de la fuerza pública, diversos análisis posteriores han señalado que parte de estos contenidos fueron difundidos de manera fragmentada, editada o descontextualizada, omitiendo elementos relevantes como la secuencia completa de los hechos o las acciones previas de los manifestantes. En consecuencia, la construcción de narrativas a partir de estos registros audiovisuales no siempre reflejó la complejidad de las interacciones en terreno. Este fenómeno ilustra cómo, en entornos informacionales altamente dinámicos, la evidencia visual puede ser utilizada selectivamente para reforzar marcos interpretativos específicos, contribuyendo a la polarización y a la disputa por la legitimidad en el dominio cognitivo.

desempeñaron un papel fundamental en la internacionalización de la protesta, organizando campañas en línea, traduciendo testimonios a varios idiomas y presionando a instituciones internacionales. Este activismo transnacional refleja patrones más amplios en las protestas latinoamericanas, donde las diásporas configuran cada vez más los movimientos nacionales a través de infraestructuras digitales (Martens et al., 2022).

Sin embargo, esta dinámica también se entrelaza con el marco estratégico de las guerras de quinta generación (G5G). En efecto, la G5G se caracteriza por tácticas no cinéticas, cognitivas y basadas en la información, donde la percepción y la influencia psicológica se vuelven centrales en el conflicto (Álvarez et al., 2017). En las protestas de 2021, existe evidencia creíble de que rivales del Estado colombiano, tanto internos como externos, utilizaron las plataformas digitales para amplificar el caos, polarizar el discurso público y erosionar la confianza de la población en las instituciones democráticas (Sanabria & Ochoa, 2021). Se hizo uso de granjas de *trolls*, cuentas de bots, así como la implementación de campañas coordinadas de desinformación disfrazadas de protesta orgánica para convertir la disidencia en un arma; esto subraya que el activismo digital puede ser cooptado por la guerra cognitiva, con el objetivo de socavar la cohesión y la seguridad nacional.

Comparativamente, se han observado en otros Estados latinoamericanos patrones similares. Por ejemplo, en Chile, las protestas del estallido social de 2019 movilizaron a millones de personas contra los modelos económicos neoliberales y la desigualdad. Las redes sociales desempeñaron un papel clave en la movilización, la creación de memes y la contextualización de la violencia estatal (Salatino, 2022). De manera parecida al caso colombiano, la juventud chilena utilizó plataformas como Instagram y TikTok para eludir los medios tradicionales y documentar las protestas. El uso simbólico del ojo como motivo de protesta (en respuesta a las heridas de balas de goma infligidas por la policía), se difundió viralmente, configurando una narrativa transmedia de resistencia.

En Nicaragua, el activismo digital ha estado vinculado a la despiadada represión estatal. Desde 2018, las protestas contra el régimen de Daniel Ortega se han enfrentado a arrestos masivos y actividades estatales de cibervigilancia; y el régimen ha adoptado el modelo del Gran Cortafuegos de China¹², implementando

¹² El "Gran Cortafuegos de China" (*Great Firewall of China*) es el nombre informal que recibe el complejo sistema de censura, vigilancia y control del tráfico de Internet implementado por el gobierno de la República Popular China como parte del Proyecto Escudo Dorado (*Golden Shield Project*). Su propósito es doble: por un lado, impedir el acceso a contenido considerado políticamente sensible o subversivo (como información sobre derechos humanos, el Tíbet, Taiwán, Tiananmen o el movimiento Falun Gong); y por otro, moldear el ecosistema

leyes para criminalizar las noticias falsas y reprimir la disidencia digital. Los activistas nicaragüenses han respondido migrando a aplicaciones cifradas y redes de la diáspora; sin embargo, la combinación de control digital autoritario y represión física ha limitado drásticamente la sostenibilidad de la movilización digital de base (Gutiérrez, 2024). En México, el activismo digital se ha convertido en un espacio clave para los movimientos feministas, las luchas indígenas y las campañas anticorrupción; por ejemplo, el activismo con hashtags como #NiUnaMenos y #NosEstánMatando ha visibilizado la violencia de género y la impunidad estatal en ese país (Moncayo, 2022). Al mismo tiempo, periodistas y activistas se enfrentan a amenazas sistémicas, como el acoso digital, la vigilancia mediante software espía (por ejemplo, Pegasus) y campañas de desinformación.

En definitiva, estas comparaciones resaltan puntos en común y divergencias. En Latinoamérica, el hacktivismo prospera en condiciones de débil confianza institucional, desigualdad sistémica y cambios generacionales hacia una política expresiva, afectiva y descentralizada. Empero, el grado de capacidad estatal para la vigilancia, la densidad de la infraestructura digital y la internacionalización de la protesta social varían, configurando trayectorias nacionales distintivas. En Colombia, las protestas de 2021 ilustran tanto el poder como la vulnerabilidad de la disidencia digital. Demuestran que las plataformas pueden ser herramientas de empoderamiento e instrumentos de manipulación.

En los últimos años, los movimientos de protesta en la región también se han convertido cada vez más en blanco de operaciones de inteligencia extranjeras destinadas a manipular a la opinión pública, exacerbar la polarización social y destabilizar a las instituciones democráticas. Estas actividades encubiertas suelen emplear sofisticadas campañas de desinformación, manipulación en redes sociales y tácticas de infiltración para influir en la trayectoria del malestar social. Como señalan académicos como Farah y Richardson (2022), los servicios de inteligencia de Estados como Rusia, China e Irán se han visto implicados en iniciativas para difundir propaganda y desinformación en toda América Latina, aprovechando las

informativo interno mediante la promoción de contenidos favorables al régimen del Partido Comunista Chino (PCC). Este sistema combina técnicas de bloqueo de direcciones IP, filtrado de palabras clave, inspección profunda de paquetes (DPI), manipulación de resultados en motores de búsqueda y plataformas sociales, así como la aplicación de algoritmos de inteligencia artificial para la vigilancia masiva predictiva. Se estima que plataformas globales como Google, Twitter, Facebook, YouTube y WhatsApp han estado bloqueadas de forma sistemática dentro del territorio chino. Además de su eficacia técnica, el Gran Cortafuegos se complementa con un aparato normativo que obliga a empresas tecnológicas y proveedores de servicios a aplicar políticas de autocensura. En conjunto, este modelo ha convertido a China en el referente mundial del autoritarismo digital y ha servido de inspiración para otros regímenes que buscan imponer su propia "soberanía informativa", como Irán, Rusia, y en América Latina, Nicaragua y Venezuela.

tensiones sociales existentes para promover sus propios intereses geopolíticos. En Chile, informes de inteligencia sugirieron que agentes extranjeros participaron activamente en la exacerbación de las protestas de 2019, con acusaciones que apuntan a la participación de agentes venezolanos y cubanos en el fomento de la violencia y el malestar (Chow & Levin, 2025).

Casos como el chileno o el colombiano ponen de relieve un patrón más amplio en el que los servicios de inteligencia extranjeros se infiltran y manipulan movimientos de protesta en toda América Latina; en efecto, al explotar los ecosistemas digitales y las vulnerabilidades sociales, estos actores foráneos buscan erosionar la confianza en las instituciones democráticas y desestabilizar las estructuras de gobernanza regional¹³. La prevalencia de estas operaciones pone de relieve la urgente necesidad de contramedidas sólidas, incluyendo protocolos mejorados de ciberseguridad, iniciativas de alfabetización mediática y cooperación internacional para salvaguardar la integridad del activismo cívico y los procesos democráticos en la región.

Ciberterrorismo: tácticas, actores y plataformas de violencia digital

La rápida digitalización de la sociedad moderna del siglo XXI ha transformado la naturaleza de las amenazas en los contextos de seguridad y defensa nacional. A medida que infraestructuras físicas se interconectan cada vez más con los sistemas cibernéticos, han surgido nuevas formas de violencia con motivaciones políticas e ideológicas. Entre ellas, el ciberterrorismo ocupa un espacio complejo y controvertido, a la vez difícil de definir y potente en cuanto a la amenaza percibida. La creciente dependencia de las tecnologías digitales para infraestructuras críticas, finanzas, gobernanza y comunicación ha ampliado la superficie de ataque para los actores estatales y no estatales, generando temores de una disrupción catastrófica inducida por los ataques cibernéticos (Weimann, 2005; Theohary & Rollins, 2015).

¹³ Por ejemplo, investigaciones periodísticas y de inteligencia reveladas por El Tiempo señalaron la existencia de un expediente conocido por agencias como la CIA, la DEA y autoridades colombianas, en el que se documenta la presencia de ciudadanos rusos en el país, así como flujos de dinero desde Moscú hacia Colombia mediante mecanismos como transferencias bancarias, criptomonedas y redes de intermediarios. Según estas investigaciones, una parte de estos recursos habría sido canalizada para apoyar acciones violentas y episodios de disturbio durante las protestas de 2019 y 2021, como lo evidencian registros audiovisuales, interceptaciones de comunicaciones y la captura de personas vinculadas a dichas redes (El Tiempo, 26 de marzo de 2022).

Conceptualización del ciberterrorismo

Si bien las actividades del hacktivismo y el ciberterrorismo implican la utilización de herramientas digitales para el logro de objetivos de naturaleza política, ambos difieren fundamentalmente en su intención, métodos y estatus normativo. Como ya se explicó, el hacktivismo se refiere al uso de técnicas de *hacking* (ataques DDoS, desfiguración de sitios web, filtraciones de datos, entre otras), para la promoción de agendas políticas o ideológicas. Con raíces en la tradición de la desobediencia civil, a menudo lo que busca es la disrupción simbólica en lugar del daño físico; esto explica porque los hacktivistas suelen atacar como forma de protesta (al menos en la mayoría de los casos), a las instituciones gubernamentales o corporaciones privadas, evitando víctimas civiles o daños a infraestructuras críticas. Acciones de grupos como Anonymous, LulzSec o RedHack suelen enmarcarse en la desobediencia civil digital, a pesar de las ocasionales ambigüedades legales que rodean sus tácticas (Jordan & Taylor, 2004).

El ciberterrorismo, por el contrario, implica ataques o amenazas con motivación política, realizados a través de sistemas o redes informáticas, con la intención de causar graves perturbaciones, causar miedo o ejercer coacción. Por ende, los diferenciadores claves frente al hacktivismo son la intención de aterrorizar, el potencial de causar daños físicos y la magnitud de la perturbación. Archer (2014) afirma que el ciberterrorismo abarca un espectro que va desde la propaganda de bajo impacto hasta ataques potencialmente devastadores contra infraestructuras críticas; por ello y a diferencia de los hacktivistas, cuyo objetivo es la visibilidad y la protesta, los ciberterroristas buscan infundir miedo y paralizar las funciones sociales o gubernamentales.

En la era de la hiperconectividad, la economía de la atención se ha convertido en el nuevo teatro de operaciones de la guerra cognitiva. Como advierte Giansiracusa (2021), las plataformas digitales no solo distribuyen información, sino que administran la percepción mediante algoritmos que maximizan el tiempo de exposición del usuario, premiando el contenido emocional, polarizante o sensacionalista. En este ecosistema mediático, el algoritmo actúa como nuevo intermediario del poder simbólico, moldeando lo que la sociedad ve, cree y teme. Por su parte, Bennett y Livingston (2021) sostienen que el colapso de las jerarquías informativas tradicionales abrió paso a un entorno de “comunicación disruptiva”, donde los flujos digitales fragmentan la verdad pública y erosionan las estructuras de autoridad. De esta convergencia surge un campo híbrido donde la información, la emoción y la percepción se entrelazan como vectores de influencia estratégica.

En este contexto, el ciberterrorismo opera en el mismo terreno que la propaganda: la economía de la atención y la vulnerabilidad cognitiva de las audiencias. Su eficacia no depende tanto del daño físico como de la capacidad de colonizar la conciencia colectiva, amplificando el miedo, la indignación o la ira a través de la viralización. Así, los ataques informacionales ya no buscan destruir infraestructuras, sino capturar la atención y desorganizar la cognición social, convirtiendo cada pantalla en un campo de batalla perceptivo. En consecuencia, el marco ético difiere, ya que mientras que el hacktivismo suele apelar a principios de justicia y transparencia, el ciberterrorismo es fundamentalmente coercitivo y se basaría en estrategias de guerra asimétrica. Además, si bien ambos fenómenos pueden compartir en común el uso de algunas técnicas (como los ataques DDoS o el *phishing*), el ciberterrorismo implicaría una mayor sofisticación y capacidad destructiva. Por lo tanto, la combinación de guerra psicológica, implicaciones cinéticas y ambigüedad estratégica sitúa al ciberterrorismo en el centro de los paradigmas de seguridad emergentes, en particular dentro del discurso de la guerra híbrida y las G5G (Weimann, 2005; Jarvis & Macdonald, 2015, Álvarez et al., 2017).

Con el fin de delimitar conceptualmente estas categorías y evitar confusiones analíticas frecuentes en la literatura especializada, la Tabla 2 sintetiza las principales diferencias entre disidencia digital, hacktivismo y ciberterrorismo en términos de motivación, medios y efectos estratégicos.

Sin embargo, la convergencia del activismo digital y la violencia requiere marcos teóricos matizados que vayan más allá de las simples dicotomías; académicos como Jarvis y Macdonald (2015) advierten contra definiciones demasiado amplias que corren el riesgo de criminalizar la protesta o justificar una vigilancia excesiva. Si bien el término cobró fuerza hacia mediados de la última década del siglo XX, especialmente en el discurso político, el consenso sobre qué es un acto ciberterrorista sigue siendo bastante fragmentado (Hardy & Williams, 2014; Jarvis & Macdonald, 2015).

Efectivamente, para algunos, la mera difusión de propaganda terrorista a través de redes sociales es un acto de ciberterrorismo; para otros, solamente los ataques a las infraestructuras críticas que lleguen a causar víctimas masivas o un colapso sistémico cumplen los requisitos para ser considerados actos terroristas. En consecuencia, la elasticidad de las definiciones ha conducido, en ocasiones, a una sobresecuritización, con voces disidentes o grupos hacktivistas etiquetados como terroristas, lo que genera preocupación por las libertades civiles (Gadish, 2017; Dilipraj, 2019).

Tabla 2. *Disidencia digital, hacktivismo y ciberterrorismo*

Criterio	Disidencia digital	Hacktivismo	Ciberterrorismo
Motivación principal	Expresión política, denuncia, oposición al poder	Activismo ideológico mediante medios digitales	Coerción política mediante intimidación y daño significativo
Marco normativo declarado	Libertad de expresión, protesta legítima	Justicia moral o causa política percibida como superior	Desestabilización, intimidación o imposición de agenda política
Relación con la legalidad	Puede ser legal o incurrir en faltas menores	Generalmente ilegal (intrusión, sabotaje digital)	Ilegal y tipificado como delito grave o terrorismo
Medios empleados	Redes sociales, blogs, campañas informativas	Defacement, filtraciones, DDoS, doxing	Ataques a infraestructuras críticas, sabotaje sistémico, daño físico indirecto
Nivel de sofisticación	Bajo a medio	Medio a alto	Alto (requiere capacidades avanzadas)
Objetivo inmediato	Visibilizar un problema o influir en opinión pública	Exponer, avergonzar o interrumpir sistemas adversarios	Generar miedo, colapso funcional o presión política estructural
Uso de la violencia	No violento (discursivo)	No violento físico, pero disruptivo digital	Puede producir daño físico indirecto o consecuencias letales
Impacto estratégico	Expresión política, denuncia, oposición al poder	Activismo ideológico mediante medios digitales	Coerción política mediante intimidación y daño significativo
Escala de efecto	Libertad de expresión, protesta legítima	Justicia moral o causa política percibida como superior	Desestabilización, intimidación o imposición de agenda política
Vinculación	Puede ser legal o incurrir en faltas menores	Generalmente ilegal (intrusión, sabotaje digital)	Ilegal y tipificado como delito grave o terrorismo

Fuente: elaboración propia.

Los orígenes del ciberterrorismo se remontan a finales del siglo XX, cuando la creciente dependencia de los sistemas de tecnología de la información generó nuevas preocupaciones sobre las amenazas asimétricas. A principios de la década de 1990, el concepto surgió en el discurso político y académico como respuesta al temor de que los grupos terroristas pudieran explotar las infraestructuras digitales para causar disrupción generalizada o miedo.

El término fue popularizado por la Corporación RAND, así como de otros centros de estudios de defensa en los Estados Unidos, a menudo enmarcado en escenarios que incluían “Pearl Harbors electrónicos” (Warren, 2008). En uno de los primeros análisis oficiales, Denning (2000) presentó el ciberterrorismo como una

convergencia del terrorismo y el cibercrimen, haciendo hincapié en la intención de causar daño o coerción. Casi al mismo tiempo, Weimann (2005) advirtió sobre una nueva forma de guerra psicológica en la que el miedo, en lugar de la destrucción física, sería el objetivo principal, advirtiendo que incluso el uso de tácticas relativamente sencillas, como la desfiguración de sitios web o el envío de correos electrónicos amenazantes, podían tener efectos desproporcionados al explotar la ansiedad pública.

El entorno de seguridad posterior a los eventos del 11 de septiembre de 2001 amplificó estas preocupaciones. Los responsables políticos y las narrativas mediáticas confundían cada vez más las ciberamenazas con el terrorismo, provocando un aumento de la financiación y la investigación centrada en el ámbito cibernético. Según Theohary y Rollins (2015), este período marcó un punto de inflexión, ya que los Estados comenzaron a incorporar el ciberterrorismo en sus doctrinas de seguridad nacional, a pesar de la ausencia de grandes ataques ciberterroristas.

A lo largo de la década de 2000, el término continuó evolucionando. Académicos como Jarvis y Macdonald (2015) argumentaron que muchas definiciones iniciales carecían de un adecuado fundamento empírico, basándose en escenarios hipotéticos en lugar de incidentes realmente observados. En su encuesta a varios investigadores, Jarvis y Macdonald (2015) encontraron una divergencia significativa en lo que constituía el ciberterrorismo, de la propaganda en línea hasta el sabotaje de infraestructuras críticas. Esta ambigüedad en la definición, si bien problemática, también reflejaba la naturaleza dinámica del panorama de amenazas.

En Europa, Archer (2014) enfatizó la utilidad política del término para moldear el discurso público y legitimar la vigilancia. De igual manera, Wilkinson y Maglaras (2023) señalan que el ciberterrorismo se ha instrumentalizado en la formación de marcos de amenazas híbridos, donde funciona como un recurso retórico para justificar operaciones cibernéticas tanto defensivas como ofensivas. Más recientemente, la aparición de grupos como ISIS ha ampliado la definición. Su amplio uso de plataformas digitales para el reclutamiento, la propaganda y la comunicación estratégica llevó a varios académicos como Lohker (2022) y Di Pietro et al. (2021) a abogar por una comprensión más amplia del ciberterrorismo, que incorpore el poder blando, la desinformación y la manipulación psicológica de audiencias transfronterizas.

Paralelamente, nuevas tecnologías disruptivas como la computación cuántica, el *blockchain* y la IA, han transformado las posibilidades operativas de los actores estatales y no estatales. Montasari (2023, 2024) analiza cómo la Cuarta

Revolución Industrial ha transformado el paradigma de las amenazas a la seguridad y defensa nacional, pasando de ciberataques aislados a ecosistemas de amenazas integrados y multidimensionales. El ciberterrorismo se entiende cada vez más no como un fenómeno aislado, sino como un componente de la guerra de la información, las operaciones híbridas y la insurgencia digital.

Entonces, y a pesar de la ausencia de una definición legal ampliamente aceptada, la amenaza estratégica del ciberterrorismo es real. Grupos como el ELN, ISIS y Hezbolá han demostrado una creciente sofisticación en el uso del ciberespacio, no solamente para la difusión de la propaganda y el reclutamiento de nuevos miembros, sino también para la planificación operativa y transacciones financieras (Lohlker, 2022; Di Pietro et al., 2021). Además, la convergencia del fenómeno del ciberterrorismo con la guerra híbrida y la guerra cognitiva ha difuminado poco a poco las fronteras entre la ciberdelincuencia, el terrorismo y la ciberguerra (Montasari, 2023; Akhgar et al., 2016). Para los autores de este capítulo, el ciberterrorismo se entiende como el uso o la amenaza del uso de los ataques informáticos para intimidar o coaccionar a gobiernos o sociedades con el fin de alcanzar objetivos políticos, religiosos o ideológicos.

Tácticas de ciberterrorismo

El ciberterrorismo, como amenaza multidimensional, abarca una amplia gama de tácticas, desde la disrupción simbólica hasta el sabotaje destructivo. A diferencia de otras formas tradicionales de terrorismo, en donde la violencia es inmediata y física, el ciberterrorismo opera a través de infraestructuras virtuales, entornos de información y dominios psicológicos. Por consiguiente, la tipificación de las tácticas de ciberterrorismo requiere un marco que incorpore tanto los medios técnicos como los efectos previstos. A partir de las investigaciones de Denning (2000), Weimann (2005), Archer (2014), Jarvis y Macdonald (2015), y avances más recientes en el análisis de amenazas (Montasari, 2023; Sampanis et al., 2023), se identifican cinco categorías tácticas del ciberterrorismo que suelen superponerse; estas categorías son: 1) ataques a la infraestructura, 2) guerra psicológica, 3) operaciones cinéticas facilitadas por medios cibernéticos, 4) reclutamiento y radicalización, y 5) apoyo financiero y logístico.

Ataques a infraestructuras críticas

Quizás la categoría más alarmante sea la de los ataques ciberterroristas contra las infraestructuras críticas, como redes eléctricas, plantas de tratamiento de agua, sistemas de control de tráfico aéreo y redes de comunicaciones. Estos ataques

buscan infundir miedo, causar interrupciones masivas o coaccionar decisiones políticas mediante la amenaza o la ejecución de la desactivación de servicios públicos clave; los sistemas SCADA (supervisión, control y adquisición de datos), encargados de gestionar numerosos procesos industriales y municipales, son particularmente vulnerables (Dilipraj, 2019). Si bien la mayoría de los ataques de alto impacto a infraestructuras hasta la fecha se han atribuido a actores estatales (como por ejemplo, Stuxnet), la posibilidad de que grupos terroristas no estatales exploten estas mismas vulnerabilidades sigue siendo una seria preocupación. Como afirman Curran et al. (2008), la disponibilidad de herramientas de control industrial de código abierto y las vulnerabilidades publicadas en foros de *hackers* reducen el umbral de acceso. Sampanis et al. (2023) clasifican estos escenarios dentro de las amenazas híbridas ciberfísicas, donde el acceso digital puede causar daños físicos o parálisis operativa.

Ataques psicológicos y simbólicos (ciberpropaganda y guerra cognitiva)

Una segunda categoría incluye acciones no letales, pero simbólicamente potentes, que buscan perturbar la confianza pública, sembrar confusión o incitar al pánico. Según Weimann (2005), estas tácticas constituyen una forma de guerra psicológica que se basa en la estética del miedo. Estas incluyen: 1) desfigurar sitios web gubernamentales o religiosos, 2) difundir mensajes terroristas o noticias falsas, 3) secuestro de narrativas en redes sociales mediante hashtags o botnets¹⁴, y 4) publicar listas de asesinatos o de personas a matar, o videos amenazantes. Ejazi (2022) enfatiza la naturaleza mediática del terrorismo moderno, donde el acto a menudo es menos importante que su visibilidad; por lo tanto, los grupos ciberterroristas buscan la viralidad, apoyándose en algoritmos de plataforma y el miedo público para amplificar su mensaje. Montasari (2024) denomina esta táctica terrorismo algorítmico, donde el impacto psicológico se maximiza mediante la ingeniería de contenido, la sincronización y la distribución.

En el terreno de la ciberpropaganda y la guerra cognitiva, la eficacia no depende solo de la capacidad técnica para difundir mensajes, sino de la ingeniería emocional y cultural que los envuelve. Las narrativas emocionales (centradas en agravios percibidos, amenazas existenciales y promesas de pertenencia), y los memes culturales (formatos visuales y audiovisuales breves, altamente replicables), actúan

¹⁴ Una botnet es una red de ordenadores y dispositivos infectados con *software* malicioso, controlada remotamente por un atacante, a menudo llamado *botmaster*, para llevar a cabo ciberataques u otras actividades maliciosas. Estos dispositivos infectados, llamados *bots*, colaboran para realizar tareas como envío de spam, la distribución de *malware* o el lanzamiento de ataques DDoS.

como amplificadores de radicalización al transformar ideas abstractas en estímulos afectivos de consumo rápido y fácil circulación en redes sociales (Nicholson et al., 2023).

Estas piezas desplazan la conversación del terreno racional al plano identitario, reforzando la idea “nosotros/ellos”, normalizando la violencia simbólica y anclando marcos interpretativos que luego habilitan conductas de apoyo, facilitación o acción directa. El estudio de Nicholson et al. (2023) muestra que esta táctica opera dentro de ecosistemas distribuidos y resilientes (no en plataformas aisladas), donde los actores extremistas adaptan su comportamiento a las oportunidades y restricciones de cada sitio para maximizar el alcance, la persistencia y la seguridad operativa.

Un elemento clave para comprender la arquitectura de estos ataques es el modelo de cinco etapas de involucramiento, que describe cómo un usuario puede pasar de una exposición inicial pasiva a una participación en la difusión de la propaganda extremista. El proceso suele comenzar con la exposición incidental, es decir, el contacto casual con contenidos extremistas en entornos digitales abiertos, muchas veces a través de memes, hashtags o videos compartidos por terceros. En esta fase, el usuario no busca deliberadamente el material, pero su presencia repetida en el entorno digital lo hace accesible y potencialmente atractivo. La segunda etapa es el consumo, caracterizada por la repetida exposición voluntaria a este tipo de contenido. Aquí, los marcos narrativos extremistas comienzan a consolidarse y las ideas violentas se normalizan, reduciendo progresivamente la resistencia psicológica hacia ellas (Nicholson et al., 2023).

En la tercera etapa, la interacción, el usuario empieza a relacionarse de manera directa con el contenido o con los propios actores extremistas. Esto puede incluir acciones como el comentar, dar “me gusta” o compartir publicaciones, lo que no solo amplifica la difusión del material, sino que también sienta las bases para vínculos iniciales con la comunidad extremista. La cuarta etapa, denominada compromiso activo, implica un grado mayor de implicación: unirse a grupos cerrados, seguir canales especializados, asistir a eventos en línea o incluso contribuir con material propio. En este punto, el individuo ya forma parte de un entorno social y comunicativo donde la ideología se refuerza constantemente.

Finalmente, la quinta etapa, defensa activa y diseminación¹⁵, se alcanza cuando el individuo no solamente adopta la narrativa extremista, sino que también

¹⁵ La defensa activa, en este contexto, es la promoción de una causa, idea o ideología, con el propósito de influir en percepciones, decisiones o comportamientos de un público objetivo.

la promueve estratégicamente (Nicholson et al., 2023). Esto incluye producir y difundir propaganda, así como desempeñar roles de “amplificador” o incluso “reclutador”, ayudando a expandir la red y atraer nuevos adeptos.

Este proceso no es estrictamente lineal, ya que los individuos pueden moverse entre etapas, permanecer en varias simultáneamente o saltar pasos. Los extremistas explotan esta flexibilidad para personalizar sus estrategias, combinando campañas de difusión masiva con *micro-targeting*¹⁶ e interacción uno a uno¹⁷. Así, el tránsito desde un meme compartido en un muro público puede derivar en una conversación directa en un canal cifrado, donde se intensifica la influencia y se construye compromiso ideológico. En términos operativos, la migración táctica de plataformas es un componente esencial; el patrón “de Twitter a Telegram” ilustra cómo las campañas captan atención en espacios visibles (con piezas emocionales, humorísticas o provocadoras), y luego dirigen a las audiencias hacia entornos cifrados para profundizar la radicalización y reducir riesgos de moderación. El caso de ISIS, que tras el endurecimiento de controles en Twitter expandió su presencia a cientos de canales en Telegram con decenas de miles de mensajes semanales, es un ejemplo paradigmático de esta táctica (Nicholson et al., 2023).

La ofuscación es otro mecanismo esencial de la guerra cognitiva. No se limita a técnicas de cifrado o alias técnicos; incluye la perfilería engañosa (por ejemplo, cuentas que se autodescriben como “periodistas independientes” para dotar de credibilidad a contenidos prorradicales), la ofuscación visual (imágenes editadas que insinúan símbolos o consignas sin gatillar detectores automáticos), así como ofuscación lingüística¹⁸ (juegos semánticos, eufemismos, variación ortográfica), con el objetivo de evadir filtros, mantener la plausibilidad negable y sostener la circulación del mensaje emocional (Nicholson et al., 2023). Estos recursos mantie-

¹⁶ *Micro-targeting* es una estrategia de segmentación que emplea datos demográficos, conductuales y psicográficos de audiencias específicas para personalizar mensajes persuasivos con alta precisión. Se utiliza ampliamente en marketing comercial, campañas políticas y, en el caso de actores extremistas, para dirigir propaganda adaptada a intereses, creencias o vulnerabilidades concretas de cada individuo o grupo, maximizando la probabilidad de influencia y conversión ideológica.

¹⁷ La interacción uno a uno hace referencia a la comunicación directa y personalizada entre un actor y un individuo, generalmente en entornos privados o semiprivados (mensajería instantánea, videollamadas, chats cifrados). En el contexto de la radicalización y el extremismo violento, esta táctica permite adaptar el discurso a las motivaciones, intereses o vulnerabilidades de la persona objetivo, estableciendo confianza y vínculos emocionales más fuertes que en interacciones públicas o masivas.

¹⁸ La ofuscación alude a la acción de entorpecer o confundir la mente, la vista o la claridad de las ideas, haciendo algo menos comprensible u ocultando información de manera deliberada. Puede manifestarse como confusión mental; deslumbramiento visual; complejización intencional de un mensaje para dificultar su comprensión; o, en el ámbito de la seguridad informática, como técnicas para ocultar código fuente o datos con el fin de proteger la propiedad intelectual o prevenir ataques.

nen la continuidad de la propaganda aun cuando se cierran cuentas o se aplican sanciones, protegiendo la cadena de influencia que va del impacto afectivo a la socialización en entornos cerrados.

La arquitectura de estos ataques psicológicos se apoya también en el *network linking*, es decir, enlazado cruzado y secuenciado dentro y entre plataformas para mover públicos desde *timelines* masivos a bots o canales con gobernanzas más laxas, y desde ahí a repositorios, *mirrors* o chats con menor trazabilidad. Este tránsito guiado asegura que el meme inicial (que puede ser humorístico, indignado o épico), sea solo el umbral de una experiencia escalonada que incorpora materiales históricos reempaquetados, “noticias” manufacturadas y llamados a la acción (Nicholson et al., 2023). En ese sentido, la desinformación es la puerta; el acompañamiento personalizado y el microenganche son el pasillo que lleva a la “sala” donde se consolidan identidad, disciplina de mensaje y lealtad.

En suma, los ataques psicológicos y simbólicos del ciberterrorismo combinan en la actualidad tanto la viralidad emocional como el diseño memético, microinteracción dirigida y migración/plataformización estratégica para moldear las percepciones, bajar las barreras morales y crear las trayectorias de radicalización que eluden contramedidas centradas solo en contenido o cuentas individuales. Abordarlos exige capacidades que lean el ecosistema como un sistema socio-técnico en flujo (atendiendo a sus etapas de involucramiento, rutas de enlace y gramáticas de ofuscación), integrando acciones preventivas, disuasivas y reactivas, coordinadas entre los ámbitos técnico, narrativo y legal; y no solo como un repositorio de piezas a moderar (Nicholson et al., 2023).

Apoyo cibernético para operaciones cinéticas

Si bien no siempre se ejecuta exclusivamente en línea, el ciberterrorismo también puede servir como facilitador del terrorismo tradicional (cinético). Esto incluye el uso de plataformas digitales para realizar reconocimiento, coordinar tiempos y amplificar el impacto. Archer (2014) se refiere a esto como la interfaz cibercinética: una convergencia donde las herramientas cibernéticas y físicas se sincronizan para lograr una eficiencia estratégica. Por ejemplo, se incluye la desactivación de la comunicación policial antes de un bombardeo coordinado, el uso de mensajes cifrados para planificar múltiples nodos de ataque o el uso de drones para la selección de objetivos.

La estructura de apoyo digital puede incluir herramientas de mapeo, vigilancia de multitudes mediante transmisiones de CCTV pirateadas o ciberintrusión para

recopilar información sobre las fuerzas de seguridad. La OTAN (2008) ha categorizado este tipo de acciones como ciberterrorismo de Nivel II, un término que designa la intensificación de las amenazas convencionales mediante medios cibernéticos.

Reclutamiento y radicalización en línea

El reclutamiento es otro componente crítico del ciberterrorismo. Grupos terroristas como ISIS han utilizado de manera extensa plataformas como X (Twitter), Telegram e incluso TikTok para difundir propaganda, glorificar el martirio y atraer nuevos adeptos (Piazza & Guler, 2021). El proceso de radicalización en línea suele ser gradual y se va construyendo mediante una narrativa que va combinando agravios étnicos, religiosos, políticos, económicos o personales en marcos ideológicos convincentes (Lohlker, 2022; Jarvis & Macdonald, 2015).

Los sistemas de recomendación basados en la IA en YouTube y Facebook pueden, sin darse cuenta, conducir a los usuarios vulnerables a ecosistemas de contenido extremista¹⁹. Estas “madrigueras” se ven amplificadas por cámaras de eco, el sesgo algorítmico y la recompensa emocional de la pertenencia al grupo (Montasari, 2023). Las tácticas de reclutamiento suelen incluir (Pashentsev & Bazarkina, 2021): 1) cuestionarios gamificados para identificar posibles combatientes²⁰, 2) revistas digitales como *Dabiq* e *Inspire*, 3) testimonios de excombatientes o víctimas, y 4) apelaciones emocionales a la comunidad, el honor o la venganza. En este contexto, una táctica particularmente insidiosa es el uso de los memes y del humor para normalizar la ideología extremista entre el público juvenil; en efecto, Ejazi (2022) ha analizado cómo los memes se han convertido en armas semióticas, difundiendo ideologías mientras enmascaran contenido radical tras imágenes de la cultura *pop*.

Disrupción financiera y financiación ilícita

El ciberterrorismo también puede implicar intentos de desestabilizar los sistemas económicos o conseguir financiación a través del cibercrimen. Estas actividades

¹⁹ Los sistemas de recomendación de IA son herramientas que utilizan algoritmos para sugerir productos, contenido o servicios a los usuarios, basándose en sus preferencias, historial de comportamiento y otros datos relevantes. Estos sistemas, que se basan en el aprendizaje automático (*machine learning*), analizan grandes cantidades de información para identificar patrones y predecir qué puede gustar a un usuario o qué podría ser de su interés.

²⁰ Los cuestionarios gamificados son cuestionarios o evaluaciones que incorporan elementos de juego, como recompensas, puntos, insignias, desafíos y competencia, para hacer el proceso de aprendizaje más atractivo y motivador.

incluyen: 1) ataques de *ransomware* y exigencia de pagos con criptomonedas, 2) campañas de *phishing* para obtener credenciales bancarias, 3) gestión de mercados ilegales en la *dark web*, y 4) lavado de dinero a través de mezcladores de criptomonedas y monederos anónimos. Gadish (2017) y Di Pietro et al. (2021) destacan cómo las organizaciones terroristas adoptan tácticas de ciberdelincuencia, en particular modelos de *ransomware* como servicio (RaaS)²¹.

Con base en lo anterior, si bien existe una superposición con la ciberdelincuencia con fines financieros, lo que distingue la financiación del ciberterrorismo es el destino ideológico de los fondos; es decir, el apoyo a la adquisición de armas, las operaciones logísticas o la difusión de propaganda. Montasari (2024) señala que viene produciéndose una creciente convergencia entre las herramientas financieras de la *dark web* y las actividades terroristas operativas; incluso las agencias de inteligencia han observado que los ciberterroristas a menudo enmascaran sus motivos como puramente delictivos para evadir el escrutinio antiterrorista.

Uso de malware, botnets y herramientas ofensivas

Más allá de las tácticas humanas, los ciberterroristas implementan herramientas automatizadas y escalables para maximizar la disrupción. Estas incluyen: 1) botnets para ataques DDoS, 2) kits de malware como BlackEnergy o Zeus, y 3) herramientas de código abierto para pruebas de penetración reconfiguradas para ataques (por ejemplo, Metasploit). Koops (2016) argumenta que la democratización del malware ha permitido a actores no estatales realizar operaciones que antes eran competencia de los Estados; estos avances sugieren una simplificación de la jerarquía de ciberamenazas, donde grupos ideológicos pueden acceder y utilizar cada vez más herramientas avanzadas.

Amenazas internas e ingeniería social

Otra táctica consiste en comprometer a personal de confianza de las instituciones que serán blanco de la acción ciberterrorista o explotar vulnerabilidades humanas. Para ello, los ciberterroristas pueden intentar: 1) campañas de *phishing* selectivo para obtener credenciales del personal de seguridad, 2) extorsionar o coaccionar a empleados con privilegios de acceso, y 3) suplantar la identidad del personal de TI o utilizar tecnologías *deepfake* para obtener acceso. Dilipraj (2019) analiza el

²¹ El *ransomware* como servicio (RaaS) es un modelo de negocio de la ciberdelincuencia en el que los desarrolladores de *ransomware* venden código *ransomware* o *malware* a otros hackers, llamados "afiliados", que luego utilizan el código para iniciar sus propios ataques de *ransomware*.

auge de la ingeniería social en el ciberterrorismo, señalando cómo la manipulación emocional, las tácticas de urgencia y la elaboración de perfiles de comportamiento se utilizan para eludir los mecanismos de seguridad tradicionales.

Las amenazas internas siguen siendo una preocupación importante, especialmente en instituciones con poca seguridad. Finalmente, cabe señalar que las categorías tácticas del ciberterrorismo que se acaban de enumerar no son mutuamente excluyentes. La mayoría de las operaciones implican estratificación táctica, donde la propaganda apoya el reclutamiento, que financia los ataques, que a su vez generan espectáculos mediáticos. Esta sinergia estratégica es un sello distintivo del ciberterrorismo contemporáneo (Tabla 3).

Tabla 3. Categorías tácticas del ciberterrorismo

Categoría táctica	Vectores de ataque	Herramientas clave utilizadas	Impacto estratégico
Ataques cibernéticos a la infraestructura	Sistemas SCADA, redes eléctricas, infraestructura crítica	Explotaciones de ICS/SCADA, herramientas DDoS, cargas útiles personalizadas	Parálisis operativa, escalada del miedo, interrupción de servicios esenciales
Ataques psicológicos / simbólicos	Desfiguración de sitios web, redes sociales, botnets, videos de propaganda	Photoshop, generadores de memes, algoritmos de desinformación	Disrupción cognitiva, control narrativo, erosión de la legitimidad estatal o institucional
Apoyo cibernético para operaciones cinéticas	Señales de CCTV, mapas digitales, drones, interferencias de comunicaciones, aplicaciones de chat cifradas	Mensajería segura, suplantadores de GPS, herramientas de vigilancia pirateadas	Violencia física sincronizada, aumento de la eficiencia operativa, multiplicación de la fuerza
Reclutamiento y radicalización	X (Twitter), Telegram, TikTok, foros de la deep web	Contenido impulsado por IA, guiones personalizados, influenciadores de propaganda	Ideología escalable, adoctrinamiento, movilización de combatientes extranjeros
Interrupción financiera y criptoфинanciación	Campañas de ransomware, kits de phishing, moneaderos de criptomonedas, mercados de la darknet	Mezcladores de bitcoin, ransomware como servicio (RaaS), plantillas de phishing	Financiación operativa, blanqueo de capitales, desconfianza financiera sistémica
Despliegue de malware y botnets	Distribución masiva de malware, infraestructuras de comando y control	Metasploit, botnets Mirai, encriptores, kits de exploits	Automatización de ataques, penetración sigilosa, disrupción escalable y repetible
Amenazas internas e ingeniería social	Suplantación de correo electrónico, coerción, suplantación de identidad, manipulación de videos deepfake	Registradores de pulsaciones de teclas, credenciales falsificadas, correos electrónicos de phishing, medios sintéticos	Violación de acceso sistémico, infiltración a largo plazo, compromiso de la confianza organizacional

Fuente: elaboración propia.

En resumen, los ataques a la infraestructura generan disrupción física inmediata, las operaciones psicológicas desestabilizan la confianza pública y amplifican el miedo, la integración cibercinética permite ataques sincronizados multidominio, el reclutamiento y la financiación sustentan la continuidad organizacional, y los kits de herramientas y la ingeniería social amplían la capacidad operativa. Sampanis et al. (2023) y Montasari (2024) concluyen que el ciberterrorismo moderno se entiende mejor como un sistema modular (flexible, descentralizado y adaptativo), capaz de explotar tanto las debilidades tecnológicas como las fisuras sociales.

Yihad digital y guerra por delegación: ISIS, Hezbolá y el ciberterrorismo estatal

El ciberterrorismo no es un fenómeno monolítico, sino un mosaico de estrategias y capacidades adaptadas a los objetivos, capacidades e ideologías de diferentes actores. Tres categorías merecen especial atención: las organizaciones yihadistas globales (como ISIS), los actores híbridos con arraigo regional (como Hezbolá), y los grupos apoyados o patrocinados por el Estado que difuminan las fronteras entre la ciberguerra y el terrorismo.

El llamado Estado Islámico (ISIS) y Hezbolá representan dos arquetipos de actores ciberterroristas cuyos fundamentos doctrinales difieren significativamente. Mientras que ISIS adoptó una agenda yihadista global arraigada en el maximalismo teológico y el espectáculo mediático, Hezbolá ha cultivado un modelo híbrido de ciberguerra arraigado en la geopolítica de Oriente Medio. Esta divergencia ha determinado el alcance, la escala y el estilo de sus operaciones ciberterroristas.

Si bien ambas organizaciones han utilizado el ciberespacio como un dominio de conflicto asimétrico, sus objetivos estratégicos han variado significativamente. En efecto, ISIS ha operado transnacionalmente, con los objetivos de inspirar a los lobos solitarios²² y construir un califato en línea desterritorializado (Lakomy, 2021; Kruglova, 2022). Hezbolá, en cambio, opera con la profundidad infraestructural que le brinda el respaldo estatal de Irán, utilizando el ciberespacio como componente de una doctrina más amplia de guerra híbrida (Besenyő et al., 2023; Warren, 2008).

Por consiguiente, las actividades cibernéticas de Hezbolá se han concentrado en la recolección de datos de inteligencia, las comunicaciones estratégicas y la disuasión psicológica, mientras que las de ISIS giran en torno a la propaganda

²² El terrorismo de "lobo solitario" se refiere a actos terroristas cometidos por individuos que actúan solos, sin pertenecer a una organización terrorista o estar bajo su dirección. La radicalización en línea es una de las causas principales del aumento de este tipo de terrorismo a nivel global.

digital, la guerra psicológica y la coordinación operativa para la movilización de partidarios a nivel global (Vacca, 2020; Lohlker, 2022). Estas diferencias enmarcan el análisis comparativo que se presenta a continuación.

ISIS: la construcción del califato virtual y la ciberyihad global

ISIS redefinió el uso del ciberespacio en el terrorismo moderno. Entre 2014 y 2018, el Estado Islámico estableció una presencia digital tan extensa que los académicos lo denominaron *califato virtual* (Lakomy, 2021). Si bien su control territorial físico ha disminuido considerablemente desde entonces, sus operaciones digitales siguen siendo un potente modelo de terrorismo en red. Como señala Lohlker (2022), la estrategia en línea de ISIS se estructuró en torno a tres pilares: difusión de propaganda, reclutamiento y radicalización, y coordinación operativa.

ISIS no era simplemente una insurgencia violenta; era una marca. Su propaganda digital enfatizaba el alto valor de producción, el alcance global y la resonancia emocional. Como señalan Vacca (2020) y Kruglova (2022), el sector mediático de ISIS, en particular el Centro de Medios Al-Hayat, produjo revistas profesionales (*Dabiq*, *Rumiyah*) y videos que combinaban la justificación religiosa con técnicas cinematográficas al mejor estilo de Hollywood. Estos materiales se dirigían no solo a los musulmanes de Oriente Medio, sino también a las poblaciones diaspóricas de Europa, Norteamérica y el Sudeste Asiático. El proceso de radicalización se producía a menudo en foros en línea semipúblicos donde la curiosidad se recibía con una preparación ideológica cuidadosamente planificada por parte de ISIS (Jarvis & Macdonald, 2015). Plataformas de redes sociales como Telegram, X (Twitter) y Facebook sirvieron como puntos de contacto iniciales, mientras que algunas aplicaciones cifradas de conversación (WhatsApp y Signal), permitieron conversaciones operativas.

De acuerdo con Lakomy (2021), la imagen de marca de ISIS se basaba en temas recurrentes: la victimización de la *ummah* musulmana, así como la lucha apocalíptica y la glorificación del martirio; y el efecto psicológico se reforzaba a través de videos de ejecuciones brutales que, si bien eran horribles, se hacían virales y se convirtieron en parte de una gramática visual transgresora que atraía a ciertas audiencias radicalizadas. Estos artefactos digitales fueron expresamente diseñados para provocar, reclutar y desestabilizar, aprovechando la lógica viral de las redes sociales (Weimann, 2005). Este ecosistema digital integrado transformó el ciberespacio en un segundo campo de batalla, uno donde las narrativas eran tan importantes como las balas.

ISIS empleó un sofisticado embudo digital para el reclutamiento. La entrada se producía a menudo a través de plataformas públicas (YouTube, Facebook, Twitter), antes de pasar a espacios cifrados como Telegram y foros de la *dark web* (Aday, 2019). El proceso de radicalización era no lineal y afectivo, y a menudo implicaba una preparación emocional personalizada, un marco ideológico y promesas de identidad, pertenencia o redención (Kruglova, 2022). Vacca (2020) destaca que los reclutadores en línea del Estado Islámico adaptaron sus enfoques en función de la geografía, el trasfondo cultural y el perfil psicográfico; esta estrategia descentralizada le permitió al grupo atraer no solo a combatientes a Siria e Irak, sino también a operativos locales en Europa, el Sudeste Asiático y Norteamérica. Ejazi (2022) identifica que la guerra de memes, la gamificación y el humor fueron herramientas de reclutamiento dirigidas a los públicos más jóvenes; y al combinar el extremismo religioso con el lenguaje subcultural, ISIS eludió las defensas ideológicas tradicionales y normalizó las creencias radicales, constituyendo poco a poco una red ciberterrorista verdaderamente transnacional.

Las operaciones cibernéticas de ISIS iban más allá de la mera comunicación. Su cibercalifato incluía *hackers* expertos capaces de lanzar ataques DDoS básicos, desfigurar sitios web y realizar campañas de *doxing*. Un ejemplo notable es el *hackeo* de 2015 a la cuenta de X (Twitter) del Comando Central de los Estados Unidos, en donde operativos afiliados a ISIS publicaron propaganda a favor del Estado Islámico. Si bien estas acciones fueron en gran medida simbólicas, tenían fines psicológicos, proyectando el alcance ciberespacial del grupo y amenazando a sus adversarios en la esfera digital (Weimann, 2005). Además, ISIS utilizó el ciberespacio para coordinar operaciones logísticas y cinéticas; los atentados terroristas de París en el 2015 revelaron cómo los atacantes utilizaban comunicaciones cifradas para planificar y ejecutar operaciones, lo que puso de relieve la interfaz ciberkinética descrita por Archer (2014) y Sampanis et al. (2023). Las herramientas cibernéticas proporcionaron anonimato, velocidad y alcance, lo que permitió que las células descentralizadas funcionaran con unidad estratégica.

Según Weimann (2011), las ciberfatwas sirvieron como justificaciones teológicas para las acciones ciberterroristas²³; estos textos instruían a los musulmanes no solo a participar en la yihad física, sino también a luchar mediante capacidades cibernéticas. Esta innovación doctrinal integró el ciberterrorismo en la esencia mis-

²³ Las ciber *fatwas* son opiniones religiosas o decisiones emitidas por eruditos islámicos (muftíes) a través de internet. Generalmente responden a preguntas sobre la ley o doctrina islámica, y pueden ser utilizadas para debates religiosos, justificación de acciones o incluso promoción de la violencia y el terrorismo.

ma de la ideología de ISIS. Montasari (2023) sitúa estos desarrollos en el contexto más amplio de la guerra de la Cuarta Revolución Industrial, donde ISIS explotó la tecnología móvil, la inteligencia artificial y las herramientas de anonimización²⁴ para construir una insurgencia virtual distribuida que trascendió la geografía.

Los efectos psicológicos del ciberterrorismo de ISIS fueron profundos. Gross et al. (2016) muestran que incluso ciberataques simbólicos pueden generar un miedo público desproporcionado; por ejemplo, la difusión de desinformación o el *hackeo* de sistemas triviales pueden percibirse como amenazas a la seguridad nacional cuando se vinculan con entidades terroristas, por lo que la omnipresencia percibida de ISIS en el ciberespacio contribuyó a un clima de hipervigilancia y ansiedad digital. La infraestructura digital de la organización también tuvo un impacto duradero en las políticas públicas, ya que catalizó el desarrollo de programas en línea contra el extremismo, como la Unidad de Referencia de Internet de la UE y el Centro de Compromiso Global en Estados Unidos; asimismo, empresas como Facebook, X y Google lanzaron sistemas de moderación de contenido para identificar y eliminar contenido extremista, a menudo haciendo uso de clasificadores basados en IA (Aday, 2019).

Incluso, la Operación *Glowing Symphony* del Comando Cibernético de Estados Unidos interrumpió la propaganda en línea de ISIS al desactivar servidores e incautar activos digitales (Di Pietro et al., 2021). Empero, estas operaciones se encontraron con limitaciones debido a problemas jurisdiccionales y a la redundancia de los sistemas de comunicación cifrados entre pares (P2P). Además, y según Pashentsev y Bazarkina (2021), una lucha exitosa contra la radicalización requiere una combinación creativa de operaciones de desmantelamiento, comunicación estratégica y otras alternativas, debido a que la simple eliminación de contenido no es suficiente; en otras palabras, las contranarrativas deben abordar los vacíos emocionales e ideológicos que llenan los mensajes de ISIS.

En definitiva, aunque las reivindicaciones territoriales de ISIS han fracasado, su legado cibernético perdura. Como señala Lakomy (2021), ISIS demostró que el terrorismo en la era digital no se limita a fronteras ni a potencia de fuego, sino a su capacidad de moldear el discurso, inspirar la acción y perdurar en código y contenido. Su yihad digital sigue siendo un caso de estudio sobre la convergencia entre la ideología, la tecnología y la guerra cognitiva, un modelo que otras organizaciones terroristas podrían replicar. La ciberestrategia de ISIS reflejó una comprensión

²⁴ La anonimización es un proceso que transforma datos personales en datos anónimos, haciendo que sea imposible identificar a una persona específica.

de la guerra de información moderna, donde la viralidad, el impacto y la resonancia emocional podían reclutar, aterrorizar y polarizar. Su guerra memética incluyó la difusión viral de videos de decapitaciones, aprovechando tanto la indignación de los medios de comunicación tradicionales como la glorificación clandestina para ampliar su influencia (Lohlker, 2022). Montasari (2023) denomina a esto sensacionalismo estratégico, es decir, el uso de la brutalidad estetizada para controlar la lógica algorítmica de las plataformas digitales.

Hezbollah: guerra híbrida y ciberterrorismo respaldado por el Estado

Hezbollah, la organización militante y partido político chií del Líbano, presenta un caso particular de ciberterrorismo que ha combinado la guerra híbrida y la estrategia geopolítica. A diferencia de ISIS, el enfoque cibernético de Hezbollah se ha caracterizado por el sigilo, la alineación con los objetivos estatales (en particular, Irán), y un enfoque estratégico en la vigilancia, el espionaje y la disuasión. Con el respaldo militar, financiero y tecnológico de Irán, Hezbollah ha integrado el ciberterrorismo en su doctrina más amplia de guerra asimétrica, manteniendo unidades cibernéticas capaces tanto de operaciones defensivas como de intrusiones ofensivas, especialmente dirigidas contra Israel y los intereses occidentales (Archer, 2014; Gadish, 2017). Por ende, su evolución como actor cibernético refleja la creciente convergencia del terrorismo, la ciberguerra y la coerción patrocinada por el Estado.

Las capacidades cibernéticas de Hezbollah están profundamente entrelazadas con la doctrina cibernética iraní. Según Warren (2008) y Besenyő et al. (2023), el grupo recibe apoyo técnico, infraestructura y capacitación del Cuerpo de la Guardia Revolucionaria Islámica de Irán (CGRI), lo que le permite operar con capacidades muy superiores a las de otros actores no estatales. Esta colaboración ha facilitado el acceso a herramientas que abarcan desde troyanos de acceso remoto (RAT) y *exploits* de día cero, hasta marcos de ingeniería social y malware de grado militar. Como señalan Di Pietro et al. (2021), la estrategia de Hezbollah incluye tanto el ciberespionaje como la disrupción psicológica, con intentos de piratear los sistemas de comunicación, las redes eléctricas y las plataformas municipales israelíes; asimismo, estas operaciones suelen incluir campañas de *phishing*, suplantación de dominios y robo de credenciales (Lakomy, 2021). Según Besenyő et al. (2023), las unidades cibernéticas de Hezbollah también han atacado periodistas libaneses disidentes y diplomáticos extranjeros, evidenciando una combinación de ciberterrorismo y tácticas de contrainteligencia.

Las operaciones ciberterroristas de Hezbolá suelen tener como objetivo aumentar las operaciones físicas o configurar entornos estratégicos mediante medios no cinéticos. Como observan Downes y Maglaras (2023), el modelo de guerra híbrida de Hezbolá incorpora herramientas cibernéticas para desorientar, desmoralizar y desestabilizar a los rivales. A diferencia de ISIS, que prospera gracias a la visibilidad, Hezbolá practica una doctrina de opacidad; esto conlleva a que sus acciones ciberterroristas suelen ser difíciles de atribuir, debido a las estructuras de negación que le ofrece el uso de intermediarios y organizaciones fantasma; esto le permite a Hezbolá distanciarse de una participación directa, conllevando que la atribución de su autoría en ciertos actos ciberterroristas sea bastante difícil. Esta estructura complica las respuestas legales y diplomáticas, ya que se sitúa en la intersección entre el terrorismo y el arte de gobernar (Kijewski et al., 2016; Downes & Maglaras, 2023), y la asimetría cibernética le permite a Hezbolá atacar mucho más allá de su teatro de operaciones inmediato, extendiendo su alcance a lugares tan lejanos como Latinoamérica. En este sentido, Archer (2014) clasifica las actividades de Hezbolá como una amenaza híbrida de nivel III, donde se entrecruzan el terrorismo, la inteligencia y la ciberguerra.

En sus operaciones, Hezbolá emplea tanto ciberescudos defensivos (protegiendo su infraestructura y finanzas ilícitas), como ingeniería social ofensiva, especialmente dentro de comunidades libanesas y chiitas de la diáspora. Según Besenyő et al. (2023), la organización implementa estrategias de reclutamiento estratificadas en internet, que incluyen educación religiosa, mentoría en línea e inducción selectiva; el reclutamiento a menudo implica establecer contacto digital a través de foros comunitarios o sitios web religiosos, seguido de una investigación presencial y adoctrinamiento ideológico. Si bien es menos visible que la radicalización televisiva de ISIS, el modelo de Hezbolá es más sostenible, ya que fomenta la lealtad mediante las relaciones personales, la integración comunitaria y la vigilancia digital.

Backes et al. (2022) sostienen que esta estrategia a largo plazo permite a Hezbolá preparar agentes para misiones especializadas, incluidas la intrusión cibernética y las operaciones financieras. En 2018, surgieron informes sobre una campaña cibernética de Hezbolá destinada a reclutar a jóvenes palestinos a través de cuentas falsas en redes sociales que se hacían pasar por activistas simpatizantes; una vez establecida la relación, estos agentes guiaban a los reclutas hacia misiones de vigilancia y sabotaje (Montasari, 2024). Esta táctica revela una forma híbrida de ciberterrorismo que combina inteligencia humana con alcance digital.

Aunque la propaganda en línea de Hezbolá es menos espectacular que la de ISIS, sigue siendo potente y muy bien cuidada. El grupo opera una constelación de sitios web, canales encriptados y medios de comunicación, como por ejemplo Al-Manar TV, que difunde sermones religiosos, mensajes políticos y glorificaciones del martirio en la “guerra santa”. Como explica Vacca (2020), Hezbolá hace uso de los medios digitales no solo para inspirar, sino también para legitimar su papel como movimiento de resistencia. Su presencia en línea fusiona temas teológicos con mensajes políticos, atrayendo tanto a simpatizantes locales como regionales. A diferencia del sensacionalismo viral de ISIS, Hezbolá emplea una estrategia de medios lentos, que enfatiza la credibilidad, el encuadre estratégico y el cultivo ideológico a largo plazo (Kruglova, 2022). Este grupo terrorista se vale de la autoridad clerical, la escatología chií y los agravios históricos para justificar sus operaciones cibernéticas, presentándolas como parte de una defensa sagrada de la *ummah*. Por consiguiente, su doctrina cibernética está diseñada para disuadir, infiltrar y desestabilizar, en lugar de conmocionar o radicalizar masivamente.

También es importante señalar que las actividades cibernéticas de Hezbolá se sustentan en una infraestructura financiera resiliente que incluye organizaciones fachada, transferencias de criptomonedas y recaudación de fondos en el extranjero. Koops (2016) destaca la capacidad del grupo para transferir fondos a través de remesas digitales, empresas fantasma y monederos electrónicos en la *dark web*. Hezbolá también ha estado implicado en otros ciberdelitos, como pagos de *ransomware* para financiar adquisiciones militares. Por consiguiente, Hezbolá ha logrado optimizar mediante el uso de plataformas digitales, comercio electrónico transfronterizo y transacciones en la red oscura (que eluden el escrutinio bancario tradicional), las cadenas de suministro para operaciones terroristas, en lo que Montasari (2023) define como *logística cibernética*.

No obstante, la capacidad ciberterrorista más formidable de Hezbolá reside en sus actividades de espionaje. En efecto, este grupo terrorista ha lanzado ataques de *phishing* selectivo contra funcionarios israelíes, personal de la ONU y periodistas regionales; estas operaciones están diseñadas no solo para la recopilación de inteligencia, sino también para coaccionar y neutralizar a sus adversarios. En varios casos documentados, Hezbolá utilizó los datos obtenidos para chantajear o exponer a sus críticos, fusionando el terror psicológico con la guerra de inteligencia (Di Pietro et al., 2021). Este enfoque refleja lo que Bjola y Pamment (2019) denominan diplomacia digital coercitiva, en la que se despliegan tácticas ciberterroristas para influir en el comportamiento político sin una escalada cinética; por lo

tanto, el dominio de Hezbolá en esta estrategia le ha permitido moldear la dinámica regional, disuadir a los adversarios y expandir su influencia bajo el radar de los umbrales de la guerra convencional.

En resumen, el paradigma ciberterrorista de Hezbolá difiere marcadamente del modelo centrado en el caos de ISIS. Ejemplifica un uso del ciberterrorismo alineado con el Estado, integrado con la inteligencia y geopolíticamente coherente. Si bien carece del carisma viral del Califato Virtual, lo compensa con profundidad operativa, ambigüedad estratégica y resiliencia infraestructural. Hezbolá representa una forma de ciberterrorismo táctico más que teatral, calculado más que catastrófico, y profundamente enredado en el equilibrio de poder regional del Medio Oriente. Demuestra cómo el ciberterrorismo puede servir como herramienta de disuasión, coerción y negociación asimétrica, lo que lo convierte en un caso de estudio crucial para comprender la fusión del terrorismo y el arte de gobernar en el ciberespacio.

Terrorismo facilitado por el Estado: líneas difusas y ambigüedad estratégica

El panorama del ciberterrorismo incluye cada vez más una categoría que difumina las fronteras convencionales entre el arte de gobernar y la insurgencia: el ciberterrorismo facilitado por el Estado. En este ámbito, los gobiernos apoyan directamente o permiten tácitamente que actores no estatales realicen operaciones cibernéticas alineadas con los intereses estatales. Este escenario crea una zona gris legal y estratégica, que desafía las nociones tradicionales de soberanía, rendición de cuentas y guerra, ya que este tipo de operaciones tienen un doble propósito: promover las agendas nacionales y, al mismo tiempo, ocultar la atribución y la responsabilidad legal. En efecto, el terrorismo de Estado no es simplemente una extensión de la política estatal, sino que a menudo opera a través del uso de actores semiautónomos, lo que permite a los gobiernos una negación plausible (Dilipraj, 2019). Estados como Rusia, Irán y Corea del Norte han estado implicados en facilitar que grupos terroristas o extremistas utilicen la infraestructura cibernética para la violencia ideológica; por ejemplo, las campañas de propaganda en el ciberespacio del Grupo Wagner durante las operaciones híbridas en África emplearon tácticas terroristas (intimidación, desinformación y ataques a la reputación), sin afiliación formal a las estructuras de seguridad del Estado (Schneider, 2022).

Como argumentan académicos como Manor y Crilley (2019) y Montasari (2023), la ambigüedad estratégica es una característica fundamental del ciberterrorismo facilitado por el Estado. Los Estados fomentan o cooptan a actores con

afiliaciones poco definidas (desde *hackers* patrióticos hasta grupos militantes), para llevar a cabo ciberataques que les proporcionen influencia geopolítica sin desencadenar declaraciones formales de guerra; estas campañas indirectas ofrecen una negación plausible, a la vez que permiten a los actores estatales ejercer coerción, disrupción y subversión.

Un ejemplo notable fue el Ejército Electrónico Sirio (EES). Aunque nominalmente era un colectivo activista pro-Assad, el EES llevó a cabo sofisticados ataques de *phishing*, desfiguración de sitios web y operaciones de vigilancia contra medios de comunicación occidentales, ONG y figuras políticas. Los analistas argumentan que el EES operaba con infraestructura, inteligencia y protección legal del régimen de Asad (Besenyő et al., 2023). Lohlker (2022) señala que las acciones del EES sirven como modelo de cómo las tácticas ciberterroristas pueden externalizarse, alineándose con objetivos estatales. Del mismo modo, las operaciones rusas en Ucrania y las campañas más amplias de guerra cognitiva en Europa han incluido operaciones de desinformación y psicológicas basadas en la ciberseguridad. Estas campañas involucran granjas de *trolls*, medios sintéticos y tácticas de suplantación digital que generan efectos terroristas, erosionando la confianza en las instituciones de gobierno y amplificando la polarización política (Di Pietro et al., 2021; Schneider, 2022).

Estos casos ponen de relieve el creciente fenómeno del ciberterrorismo estatal, en el que los Estados subcontratan la guerra ideológica a actores no estatales, que suelen contar con el apoyo estatal de herramientas de malware, informes de inteligencia y refugio seguro. Los Estados suelen recurrir a las amenazas persistentes avanzadas (APT), que son sofisticadas cadenas de malware y *exploits* típicamente asociadas con comandos cibernéticos nacionales; estas APT se difunden a través de intermediarios externos, como organizaciones terroristas o células cibernéticas con afinidades ideológicas. Por ejemplo, las APT33 y APT35 de Irán han compartido herramientas con operativos de Hezbolá y los hutíes. Según Sampanis et al. (2023), estas APT proporcionan sigilo, persistencia y acceso sistémico que permiten a estos actores atacar sistemas de alto valor como plantas de tratamiento de agua, instituciones bancarias y control del tráfico aéreo.

El resultado, en consecuencia, es una alineación estratégica entre las capacidades estatales de ciberguerra y las motivaciones ciberterroristas. En Corea del Norte, unidades cibercriminales como el Grupo Lazarus se han vinculado a campañas de *ransomware* que simultáneamente financian intereses estatales y apoyan insurgencias subsidiarias en zonas de conflicto. Estas operaciones difuminan

la línea entre ciberdelincuencia, guerra y terrorismo, lo que Dilipraj (2019) denomina un espectro híbrido de coerción. Por su lado, Curran et al. (2008) lo clasifican como ciberterrorismo escalonado, reflejando una complejidad creciente según el grado de participación de los actores estatales. Además, el uso estratégico de agentes ciberterroristas permite a actores estatales instrumentalizar narrativas ideológicas en regiones donde la fuerza convencional podría provocar una reacción diplomática adversa. Entonces, la flexibilidad operativa de estos agentes permite la manipulación encubierta del ecosistema de información digital, lo que puede producir efectos terroristas sin atribución directa (Montasari, 2023; Wilkinson & Maglaras, 2023).

El ciberterrorismo estatal también explota cada vez más el desorden informativo, que abarca tanto la desinformación como la información errónea²⁵. Las campañas de guerra cognitiva originadas en Estados como Irán, Rusia, China, Nicaragua y Venezuela han hecho uso de narrativas manipuladas, imágenes sintéticas y filtraciones de datos para fomentar o exacerbar el malestar, sembrar la duda y aterrorizar a la población propia o adversaria, por lo que estas operaciones psicológicas suelen reflejar tácticas terroristas tradicionales, como el miedo, confusión y espectáculo. Según Gross et al. (2016), el impacto social de estas campañas puede rivalizar con los ataques físicos en términos de desestabilización. El miedo inducido por suplantaciones de identidad digitales (por ejemplo, transmisiones de emergencia falsas), puede llegar a causar pánico público, desconfianza en el gobierno y cambios de comportamiento entre el personal crítico.

El terrorismo de Estado prospera en la zona gris, el espacio entre la paz y la guerra, donde las normas legales y estratégicas siguen siendo ambiguas. Estados como Irán, China y Rusia mantienen milicias cibernéticas, es decir, redes de actores, estudiantes y tecnólogos con motivaciones ideológicas que reciben entrenamiento y equipo estatal mientras operan extraoficialmente. Estos grupos pueden iniciar campañas que incluyen ataques DDoS dirigidos a sistemas financieros, acoso a periodistas mediante *deepfakes*, ciberchantaje a disidentes políticos, y reclutamiento de mercenarios o *hackers* en la *dark web*. Pero una característica definitoria del ciberterrorismo facilitado por el Estado es su capacidad para evadir los regímenes políticos mediante el blanqueo normativo; esto se refiere al uso de definiciones ambiguas, jurisdicciones legales contradictorias y retórica política

²⁵ La "información errónea" se da cuando la información es incorrecta, inexacta o falsa, pero no necesariamente intencionalmente engañosa. La "desinformación" es cuando la información es intencionalmente falsa o engañosa, con el propósito de manipular o engañar a las personas.

para legitimar u ocultar la ciberagresión. En efecto, los Estados pueden presentar las acciones cibernéticas con fines terroristas como hacktivismo patriótico o defensa de la información, lo que debilita la respuesta internacional (Ariely, 2008; Archer, 2014). Además, estos Estados suelen explotar las limitaciones del derecho internacional, que carece de consenso sobre la atribución de las operaciones cibernéticas y la misma definición del ciberterrorismo. En consecuencia, los Estados atacados tienen dificultades para formar coaliciones e implementar sanciones a los atacantes, sin pruebas definitivas de la complicidad estatal.

En conclusión, el ciberterrorismo facilitado por los Estados representa una clara convergencia de la asimetría y la ambigüedad. Comprender este modelo es crucial para las futuras estrategias de contrterrorismo y ciberdefensa. Requiere marcos de atribución cibernética mejorados, coordinación jurídica transfronteriza y la redefinición de las doctrinas de disuasión para dar cuenta de los intermediarios digitales y las campañas encubiertas que ahora dominan el panorama del ciberterrorismo.

Emprendedores de la violencia

Finalmente, una figura emergente en el ecosistema del ciberterrorismo es la del emprendedor de la violencia, es decir, individuos o microcolectivos que, sin un aparato jerárquico tradicional, explotan las lógicas de las plataformas de redes sociales para construir microcomunidades extremistas altamente cohesionadas y operativamente útiles. Su valor estratégico reside en ocupar el nivel “meso” entre el lobo solitario y la organización formal; en otras palabras, se constituyen como nodos catalizadores que convierten audiencias difusas en bases militantes, ensamblando identidades, repertorios tácticos y canales de coordinación con costos fijos muy bajos. Lejos de actuar de modo errático, estos actores siguen patrones adaptativos, como ofuscación (lingüística, visual y de perfilera) para evadir moderación; selección de plataformas según tolerancias y riesgos; vinculación en red (*network linking*), para encadenar espacios abiertos con entornos cifrados; y compromiso de contenido (repaquetado, reciclaje y curaduría), para mantener atención y fidelidad (Nicholson et al., 2023).

Analíticamente, su desempeño se entiende mejor como emprendimiento político-mediático, puesto que usan métricas de atención (seguidores, *reposts*, retención), y estrategias de captura de audiencia para optimizar narrativas y formatos (memes, clips breves, hilos), desplazando el procesamiento cognitivo hacia lo afectivo. En este sentido, operan como productores-analistas que detectan

ventanas de oportunidad discursivas, testean marcos emocionales y estandarizan aquello que muestra mayor efectividad. Conectan además la difusión masiva con la conversación personalizada, combinando micro-targeting con interacción uno a uno para llevar a los usuarios ambiguos desde la exposición incidental hasta la defensa y diseminación activa, reproduciendo el modelo de cinco etapas de involucramiento en trayectorias de radicalización personalizadas y no lineales. Este rol de agregadores-puente se fortalece mediante el uso de plataformas intermedias que funcionan como espacios de tránsito inicial antes de canalizar a los usuarios hacia entornos cerrados como Telegram, Element o Discord. En estos espacios restringidos, los actores extremistas consolidan la disciplina del mensaje, establecen mecanismos de control de acceso y mantienen una coordinación operativa sostenida (Nicholson et al., 2023).

A diferencia de las organizaciones formales, los emprendedores de la violencia despliegan estructuras flexibles, como marcas personales y microrredes que se reconfiguran tras sanciones o cierres, conservando comunidad mediante migraciones coordinadas y sistemas de redundancia (*mirrors*, canales alternos, listas de distribución). Su resiliencia no depende de la infraestructura propia, sino de competencias (curaduría, diseño memético, gestión de reputación, seguridad operacional), acopladas a cualidades de las plataformas (como los algoritmos de recomendación, mensajería cifrada, o los APIs²⁶). Funcionalmente, operan como *brokers* que maximizan centralidades de intermediación en el grafo sociodigital, ya que enlazan comunidades y traducen marcos ideológicos a códigos locales (memes, humor, agravios específicos), logrando acelerar la movilización simbólica hacia acciones de facilitación (financiamiento cripto, *doxing*, sabotaje digital leve), o la coordinación con actores más capaces.

Para la respuesta estatal, conceptualizarlos como unidades emprendedoras (y no meros usuarios o *influencers*) tiene implicaciones estratégicas, ya que desplaza el foco desde el contenido aislado hacia cadenas de enlace y mecanismos organizativos que sostienen la radicalización. En términos de la política pública y el contraterrorismo, su neutralización exige combinar: 1) inteligencia de ecosistemas (mapeo de rutas de enlace y nodos puente), 2) intervención algorítmica y

²⁶ Una Application Programming Interface (API) o "Interfaz de Programación de Aplicaciones", es un conjunto estandarizado de reglas, protocolos y herramientas que permiten la comunicación y el intercambio de datos entre diferentes sistemas o programas. En el contexto de plataformas digitales, las API facilitan la extracción de datos, la automatización de interacciones y la integración con servicios externos, pudiendo ser utilizadas tanto con fines legítimos (por ejemplo, investigación y desarrollo de aplicaciones) como maliciosos (por ejemplo, automatización de propaganda o monitoreo de objetivos).

gobernanza de plataformas (para romper itinerarios estándar de migración y canalización), y 3) contramedidas narrativas situadas, capaces de desacoplar la relación emprendedor–comunidad y degradar la ventaja comparativa que extraen de la atención, la personalización y la ofuscación (Nicholson et al., 2023).

Plataformas digitales del ciberterrorismo y la Cuarta Revolución Industrial

Como ya se ha mencionado en secciones anteriores, la infraestructura operativa del ciberterrorismo se construye cada vez más sobre plataformas digitales diseñadas originalmente para la apertura, el anonimato y la conectividad global. Desde los flujos virales de las redes sociales hasta las redes cifradas de la *dark web*, los ciberterroristas explotan estos sistemas para la propaganda, el reclutamiento, la comunicación y el apoyo financiero. En consecuencia, plataformas de redes sociales como X (Twitter), Facebook, YouTube y TikTok se han convertido en escenarios fundamentales del ciberterrorismo contemporáneo. Estas plataformas sirven no solo como megáfonos para la comunicación ideológica, sino también como teatros de operaciones dinámicos: sitios donde el reclutamiento, la incitación y la difusión de propaganda ocurren en tiempo real.

ISIS, en particular, demostró cómo utilizar las redes sociales como arma para establecer un califato digital. Como explica Lakomy (2021), el uso de Twitter por parte del grupo para distribuir propaganda y conectar con sus seguidores transformó la plataforma en un ecosistema semiautónomo de radicalización. Operativos y simpatizantes de ISIS utilizaron hashtags de tendencia, bots automatizados y elementos visuales con gran carga emocional para atraer a audiencias mucho más allá de los círculos yihadistas tradicionales (Vacca, 2020; Kruglova, 2022). La interacción de Hezbolá en redes sociales es más selectiva y está más alineada con el Estado. Emplea canales semioficiales, afiliados a medios de comunicación (por ejemplo, Al-Manar), y académicos religiosos para reforzar su legitimidad y autoridad moral. En lugar de la viralidad, Hezbolá prioriza la credibilidad y el enfoque estratégico, integrando su narrativa en el discurso más amplio de la resistencia chií (Besenyo et al., 2023). La expansión global de los videos cortos en TikTok ha dado lugar a un nuevo estilo de guerra memética, en donde los mensajes terroristas se codifican con humor, música o mezclas visuales; estos formatos son particularmente eficaces para llegar a los grupos demográficos más jóvenes y eludir los algoritmos tradicionales de moderación de contenido (Gelici, 2022).

Tras el aumento de los esfuerzos de las empresas de redes sociales por eliminar plataformas, muchos ciberterroristas han migrado a servicios de mensajería cifrada como Telegram, Signal, Threema y WhatsApp. Estas plataformas ofrecen cifrado de extremo a extremo, funciones de coordinación de grupos y un anonimato relativo. Telegram, en particular, se ha convertido en la columna vertebral de la logística digital yihadista. Alberga grupos de reclutamiento, debates tácticos en directo y contenido ideológico. Canales como Nashir News sirven de canales de propaganda de facto para ISIS y sus afiliados, operando bajo un ciclo continuo de desmantelamiento y reaparición (Lakomy, 2021). Montasari (2023) y Sampanis et al. (2023) señalan que estas aplicaciones no solamente sirven como herramientas de comunicación, sino también como repositorios de conocimiento doctrinal, incluyendo manuales para la fabricación de bombas, el ciberfraude y la evasión operativa. Los grupos emplean mensajes autodestructivos, archivos cifrados y capas de VPN para garantizar la resiliencia y la redundancia. El uso de aplicaciones cifradas por parte de Hezbolá es similar al de las unidades cibernéticas estatales. La mensajería cifrada se ha utilizado para la transmisión de comandos, la coordinación de la vigilancia e incluso la difusión ideológica a través de redes clericales (Besenyő et al., 2023).

La *dark web* proporciona a los ciberterroristas una infraestructura persistente para la comunicación anónima, transacciones financieras y coordinación logística. Consiste en servicios ocultos alojados en plataformas como Tor, I2P y ZeroNet, que anonimizan el tráfico de usuarios y ocultan la ubicación de los servidores. Los grupos afiliados al ISIS han utilizado foros de la *dark web* para entrenamiento, adoctrinamiento ideológico e intercambios en el mercado negro. Como destaca Vacca (2020), estos foros albergan ciber fatwas, guías de martirio y planes operativos. Las actividades financieras incluyen el lavado de criptomonedas, los pagos de *ransomware* y la adquisición de armas.

La presencia de Hezbolá en la red oscura es menos llamativa, pero estratégicamente robusta. La utiliza para el lanzamiento de inteligencia, la transferencia de datos de vigilancia y la comunicación con agentes encubiertos en el extranjero. Di Pietro et al. (2021) y Besenyő et al. (2023) documentan billeteras vinculadas a Hezbolá en servicios de mezcla de Bitcoin, lo que sugiere una profunda integración en la economía sumergida de criptomonedas. La *dark web* también alberga ciberterrorismo como servicio, donde herramientas como cargas útiles de malware, botnets y kits de *phishing* se pueden adquirir de forma anónima. Esto reduce la

barrera de entrada para actores menos sofisticados y permite operaciones terroristas escalables (Kijewski et al., 2016).

Por lo tanto, la instrumentalización de las características de las plataformas (como los hashtags, motores de recomendación, protocolos *peer-to-peer*), ilustra un nuevo modo de adaptación estratégica que desafía los paradigmas de seguridad tradicionales. Combatir eficazmente el ciberterrorismo en el entorno digital requerirá más que la eliminación de plataformas y las prohibiciones. Exige estrategias adaptativas de contraplataformas, colaboraciones público-privadas y una gobernanza multisectorial que preserve los derechos digitales y niegue a los extremistas violentos las ventajas de las plataformas globales.

Un patrón recurrente en la ecología digital del extremismo violento es la migración progresiva de usuarios desde plataformas abiertas y de gran alcance (como Facebook o Twitter/X), hacia entornos cerrados o cifrados, entre los que destacan Telegram, Discord y foros especializados. Esta transición obedece, en gran medida, a la presión ejercida por políticas de moderación y vigilancia en las redes masivas, que obliga a los actores extremistas a buscar espacios con mayor control sobre la visibilidad y el acceso²⁷. En este proceso desempeñan un papel clave las plataformas puente (*bridge platforms*), concebidas como zonas grises que no presentan, al menos en apariencia, un contenido explícitamente violento, pero que facilitan el reclutamiento inicial y la construcción de afinidades. En estas plataformas intermedias (que pueden incluir canales de YouTube, cuentas de TikTok o subforos de Reddit), los extremistas publican material con carga ideológica moderada, memes culturales y narrativas emocionales diseñadas para atraer a audiencias susceptibles sin activar mecanismos inmediatos de censura (Nicholson et al., 2023).

Este tránsito no es aleatorio, sino que reproduce de forma adaptativa el modelo de cinco etapas de involucramiento, que ya se describió anteriormente. En la exposición incidental, las redes masivas ofrecen la primera interacción casual con mensajes o símbolos extremistas. La fase de consumo repetido se desarrolla en plataformas puente, donde el usuario encuentra contenido reiterado que refuerza

²⁷ El extremismo violento se refiere a la adhesión y promoción de ideologías radicales que justifican o legitiman el uso de la violencia para alcanzar fines políticos, religiosos o ideológicos. Incluye tanto acciones físicas (atentados, violencia organizada) como digitales (propaganda, incitación), pero no necesariamente implica el uso de ciberataques. El ciberterrorismo, en cambio, es una modalidad específica de terrorismo que emplea medios digitales para producir efectos terroristas directos (como ataques a infraestructuras críticas, sabotajes de sistemas o denegación de servicios), o indirectos (como campañas de propaganda o amenazas). Mientras que el extremismo violento describe la motivación ideológica, el ciberterrorismo describe el medio y la táctica. Ambos fenómenos pueden converger cuando actores extremistas utilizan tácticas cibernéticas para materializar su agenda violenta.

marcos narrativos y normaliza ideas violentas. La interacción y el compromiso activo ocurren cuando la persona comienza a participar en comunidades cerradas, seguir canales dedicados y entablar diálogos dirigidos mediante el micro-targeting o las interacciones uno a uno. Finalmente, en la fase de defensa activa y diseminación, los entornos cifrados sirven como base para la producción y distribución estratégica de propaganda, consolidando disciplina de mensaje, control de acceso y coordinación sostenida. De este modo, el uso escalonado de plataformas refleja un modelo convergente de herramientas, en el que los entornos masivos, las zonas intermedias y los canales cifrados funcionan como un único ecosistema articulado para maximizar el alcance, resiliencia e impacto propagandístico de la actividad ciberterrorista.

Pero a medida que avanzamos hacia una era marcada por el cambio tecnológico exponencial, el futuro del ciberterrorismo también estará determinado por la convergencia de la inteligencia artificial (IA), los sistemas autónomos y la dinámica de la guerra híbrida. La Cuarta Revolución Industrial (4RI), caracterizada por la fusión de sistemas digitales, biológicos y físicos, proporciona nuevas herramientas, objetivos y terreno para las actividades ciberterroristas. En efecto, la IA es un arma de doble filo en el ámbito del ciberterrorismo, ya que si bien mejora la ciberseguridad mediante detección automatizada de amenazas y el análisis de anomalías, también ofrece a ciberterroristas la capacidad de desarrollar *malware* adaptativo, engaños basados en *deepfakes* y orquestación de ataques en tiempo real.

Montasari (2024) advierte sobre el ciberterrorismo potenciado por IA, en el que se utilizan modelos de aprendizaje automático para identificar vulnerabilidades, diseñar campañas de *phishing* selectivo o simular el comportamiento humano para infiltrarse en los sistemas. Los grupos terroristas también pueden utilizar herramientas de IA generativa para producir propaganda a gran escala, traducir contenido a diferentes idiomas o personalizar narrativas de reclutamiento. La tecnología *deepfake* presenta un vector particularmente insidioso; como señalan Wardle y Derakhshan (2017) y Kearns (2019), los medios sintéticos pueden utilizarse para suplantar a líderes políticos, difundir falsas declaraciones de guerra o inventar reivindicaciones terroristas, difuminando la línea entre ficción y realidad en crisis en tiempo real.

Aunque aún es emergente, la computación cuántica plantea riesgos a largo plazo para la seguridad digital. La capacidad de las máquinas cuánticas para romper los estándares actuales de cifrado podría hacer que infraestructuras críticas, bases de datos de inteligencia y sistemas financieros sean vulnerables a la

exfiltración o interrupción por parte de actores hostiles, incluyendo agentes ciberterroristas (Demertzis et al., 2023).

Los actores híbridos respaldados por Estados podrían ser los primeros en utilizar las capacidades poscuánticas como arma, pero la difusión de las tecnologías cuánticas podría eventualmente empoderar a grupos no estatales para desafiar los equilibrios de poder asimétricos. Asimismo, la fusión de la biotecnología y sistemas digitales introduce nuevas vulnerabilidades. Los implantes médicos inteligentes, los dispositivos médicos portátiles y las interfaces cerebro-computadora (BCI) son potencialmente susceptibles a la ciberintrusión. En teoría, los terroristas podrían atacar marcapasos, bombas de insulina o dispositivos neuronales para inducir daños o crear situaciones de toma de rehenes. Si bien aún son especulativos, académicos como Gadish (2017) argumentan que estos escenarios exigen una regulación preventiva y la integración de la bioseguridad en la planificación de la ciberseguridad. El terrorismo puede evolucionar para explotar no solo la infraestructura o la información, sino también la integridad biológica de las personas.

Las G5G (el uso integrado de la fuerza convencional, tácticas irregulares y operaciones de información), ya es una característica definitoria de los conflictos del siglo XXI (Álvarez et al., 2017). El ciberterrorismo se integra cada vez más en este modelo como una capa táctica que se despliega junto con la desinformación, el sabotaje económico y la militancia por delegación; el ciberterrorismo facilitado por los Estados representa la vanguardia de esta fusión, en donde los grupos terroristas alineados con patrocinadores estatales se despliegan como insurgentes digitales para erosionar la confianza pública, perturbar funciones críticas o exacerbar las tensiones sectarias en Estados rivales (Di Pietro et al., 2021; Akhgar et al., 2016).

En el ámbito defensivo, las fuerzas del orden recurren cada vez más al análisis predictivo basado en IA para detectar la radicalización, mapear redes de amenazas y anticipar ataques. Estas herramientas analizan el comportamiento en redes sociales, los metadatos y los patrones de comunicación para identificar a actores sospechosos. Si bien es prometedor, este enfoque plantea cuestiones éticas en relación con el sesgo, la elaboración de perfiles y el debido proceso. Como advierten Jarvis et al. (2014), los sistemas predictivos deben ser transparentes, responsables y estar complementados con el criterio humano para evitar reforzar las desigualdades sistémicas o generar falsos positivos.

Por último, la descentralización del ciberpoder implica que la gobernanza futura requerirá una regulación policéntrica que involucre a Estados, corporaciones,

sociedad civil y tecnólogos. La proliferación de sistemas autónomos, plataformas descentralizadas y tecnologías financieras irrastreables desafiará los regímenes regulatorios existentes. Con relación a lo anterior, Lakomy (2021) enfatiza la importancia de la “soberanía digital sin autoritarismo”, sugiriendo que los marcos antiterroristas deben salvaguardar tanto la seguridad como la arquitectura abierta de internet. Los acuerdos internacionales sobre tecnologías emergentes, especialmente la IA y la criptografía, son esenciales. Por lo tanto, el futuro del ciberterrorismo estará marcado por la sofisticación tecnológica, la hibridación doctrinal y la complejidad normativa. Y la próxima ola de amenazas no surgirá únicamente de enclaves extremistas, sino también de las interacciones entre la IA, el caos informativo y la hipervelocidad. Contrarrestarlas va a requerir previsión, claridad ética e innovación doctrinal y normativa.

Desafíos legales y respuestas a la amenaza del ciberterrorismo

El análisis de ISIS, Hezbolá y el ciberterrorismo estatal revela paradigmas distintos en doctrina, alcance operativo, selección de objetivos e integración tecnológica. Si bien los tres casos de estudio que se revisaron abordan el ciberespacio como un ámbito de disputa, las estrategias de ISIS, Hezbolá y las milicias terroristas patrocinadas por los Estados reflejan fundamentos ideológicos, infraestructurales y geopolíticos diferentes.

Por ejemplo, ISIS ejemplifica el ciberterrorismo ideológico de alta intensidad. Por lo tanto, su enfoque es transnacional, viral y performativo, aprovechando algoritmos de redes sociales, brutalidad estética y resonancia emocional para reclutar y radicalizar a nivel global. Sus operaciones digitales (que abarcan desde la guerra de memes hasta la coordinación cifrada), demuestran cómo el terrorismo puede desarrollarse a través de nodos, no de territorios (Lakomy, 2021; Kruglova, 2022). En otras palabras, el objetivo estratégico de ISIS es la disrupción, no la sostenibilidad; es el impacto, no el secretismo.

En cambio, Hezbolá encarna una asimetría híbrida, es decir, fusiona capacidades cibernéticas con el arte de gobernar, el espionaje y la disuasión psicológica. Su uso del ciberespacio es quirúrgico, no espectacular. Con el apoyo de Irán, el ciberterrorismo de Hezbolá se enmarca en una lógica geopolítica más amplia de resistencia, disuasión e influencia (Besenyő et al., 2023; Vacca, 2020).

Representa una forma de ciberterrorismo estratégico, arraigada en la coerción calculada, la infiltración persistente y la legitimidad ideológica. Por otra parte, el ciberterrorismo facilitado por los Estados introduce una tercera dimensión, la ambigüedad como doctrina. Externaliza los objetivos estatales a través de intermediarios, difumina la atribución y utiliza la negación como arma. Esta forma de ciberterrorismo utiliza el desorden informativo, la manipulación de *deepfakes* y la guerra de datos coercitiva para desestabilizar a los oponentes sin una confrontación directa (Montasari, 2023; Di Pietro et al., 2021).

En los tres ámbitos, el ciberespacio funciona no solo como una herramienta, sino como un ecosistema: un medio a través del cual circulan el afecto, las creencias y el miedo. Estos actores demuestran que el ciberterrorismo no se limita al sabotaje de sistemas; abarca la guerra cognitiva, la infiltración digital, la disrupción financiera y el contagio afectivo. ISIS, Hezbolá y los grupos estatales reflejan la naturaleza plural del ciberterrorismo en el siglo XXI. Ilustran cómo el ciberespacio está siendo colonizado por ideologías violentas, campañas encubiertas y disuasión estratégica. Comprender sus tácticas distintivas y superpuestas no es solo un ejercicio académico, sino fundamental para el desarrollo de estrategias anticiberterroristas resilientes, éticas y eficaces en una era de conflicto digital.

Por consiguiente, los marcos de seguridad deben distinguir entre el ciberterrorismo ideológico (ISIS), actores híbridos estratégicos (Hezbolá) y asimetrías de los Estados intermediarios (Rusia, Irán). Cada uno exige contramedidas únicas, desde la lucha contra la radicalización hasta la contrainteligencia digital y el desarrollo de tratados. Asimismo, los protocolos de atribución mejorados, incluyendo la investigación forense digital asistida por IA y la cooperación internacional en inteligencia de amenazas, son esenciales para identificar a los actores encubiertos facilitados por el Estado y prevenir la escalada de represalias. Finalmente, las normas jurídicas existentes son inadecuadas. Una doctrina revisada sobre los ciberconflictos (codificada a través de la Convención de Budapest o los procesos del Grupo de Expertos Gubernamentales de las Naciones Unidas), debe abordar explícitamente la complicidad estatal en el ciberterrorismo y establecer umbrales para la violación de la soberanía.

En efecto, una de las barreras más persistentes para combatir eficazmente el ciberterrorismo reside en el problema de la atribución: la dificultad de identificar, con alta fiabilidad, la responsabilidad de una determinada operación cibernética. La ambigüedad de las firmas digitales, el uso de servidores *proxy* y la facilidad para falsificar direcciones IP dificultan la atribución no solo técnicamente, sino también

políticamente. Además, la ausencia de marcos legales armonizados agrava estas dificultades, creando vacíos prácticos y normativos en la gobernanza cibernética.

La atribución en el ámbito cibernético requiere una combinación de análisis forense técnico, análisis del comportamiento y fusión de inteligencia. Sin embargo, como señala Denning (2000) y reitera Jarvis y Macdonald (2015), las operaciones cibernéticas pueden llevarse a cabo de forma anónima, utilizando banderas falsas o herramientas compartidas entre grupos de actores. Las organizaciones terroristas aprovechan esta opacidad para desviar la culpa y dificultar las represalias.

Por ejemplo, tanto ISIS como los colectivos hacktivistas pro-Assad han utilizado kits de explotación de código abierto, lo que dificulta determinar si un ciberataque determinado proviene de una célula terrorista, un actor deshonesto o un agente estatal (Kijewski et al., 2016; Montasari, 2023). La falta de consenso sobre qué constituye prueba suficiente de atribución ha minado las respuestas internacionales y retrasado las sanciones colectivas (Downes & Maglaras, 2023).

Ambigüedad jurídica y jurisdiccional en torno al ciberterrorismo

Hasta 2025, ningún tratado global define el ciberterrorismo de forma vinculante, y el Convenio de Budapest, si bien aborda los ciberdelitos de forma amplia, carece de disposiciones específicas sobre los ciberataques con motivación ideológica. Este vacío de definición conduce a una aplicación inconsistente de las leyes nacionales. Como argumentan Archer (2014) y Gadish (2017), algunos Estados han utilizado la etiqueta de ciberterrorismo para justificar la represión de la disidencia o la oposición política, lo que plantea preocupaciones en materia de los derechos humanos. Además, la fusión del terrorismo, el ciberdelito y la guerra complica la jurisdicción. ¿Un ataque a la red eléctrica constituye un acto de guerra o un acto de terrorismo?; si una campaña de desinformación de un Estado extranjero desestabiliza las elecciones políticas en otro Estado, ¿constituye una violación de la soberanía? Estas preguntas siguen sin resolverse y están abiertas a la interpretación política.

Además, el ciberterrorismo, por naturaleza, trasciende las fronteras nacionales; y ocurre que los perpetradores pueden residir en un país, dirigir el tráfico a través de otro y atacar a las víctimas en un tercero. Esta dispersión geográfica crea enormes desafíos para la aplicación jurisdiccional; los tratados de asistencia legal mutua suelen ser lentos, y la cooperación entre las fuerzas del orden se ve usualmente obstaculizada por las prioridades divergentes, falta de confianza y leyes de protección de datos incompatibles (Mercado, 2008). El caso de reclutadores de

ISIS que operan desde Alemania mientras atacan a personas en Canadá a través de Telegram ejemplifica este problema. Si bien cada Estado puede considerar la conducta ilegal, el proceso de enjuiciamiento implica una larga diplomacia y análisis forense digital que puede verse obstaculizada por el cifrado o la falta de cooperación de la plataforma.

Si bien la adopción generalizada del cifrado de extremo a extremo ha protegido la privacidad del usuario, también ha complicado los esfuerzos para detectar y enjuiciar las actividades ciberterroristas. Plataformas como Telegram, Signal y WhatsApp se resisten a conceder a las fuerzas de seguridad de los Estados el acceso por puerta trasera²⁸, alegando derechos de los usuarios y las protecciones constitucionales a la privacidad. Entonces, mientras los gobiernos presionan para que se establezcan mandatos legales para acceder a datos cifrados, las empresas tecnológicas se resisten, temiendo daños a la reputación y a la vulnerabilidad técnica. Como argumenta Ariely (2014), lograr un equilibrio entre seguridad y libertad es uno de los dilemas éticos centrales en la cibergobernanza moderna, ya que la vigilancia excesiva corre el riesgo de tener efectos disuasorios sobre la libertad de expresión, y puede llegar a ser utilizada como arma por regímenes autoritarios.

Los esfuerzos para codificar las normas internacionales sobre ciberterrorismo han sido lentos, pero están evolucionando. El Grupo de Expertos Gubernamentales de las Naciones Unidas (GGE) y el Grupo de Trabajo de Composición Abierta (GTCA) han avanzado en la promoción del comportamiento responsable de los Estados en el ámbito ciberespacial, pero estos marcos no son vinculantes y todavía adolecen de mecanismos de aplicación. Wardle y Derakhshan (2017) afirman que la iniciativa normativa de coaliciones regionales, como por ejemplo, la Ley de Servicios Digitales de la UE y la Convención sobre Ciberseguridad de la Unión Africana, pueden ofrecer modelos para una adopción más amplia; empero, las tensiones geopolíticas, especialmente entre potencias cibernéticas como Estados Unidos, China y Rusia, han frenado el consenso.

Respuestas estratégicas en EE. UU., el Reino Unido, la OTAN y el sur global

La complejidad del ciberterrorismo requiere respuestas estratégicas a medida, adaptadas a los perfiles de riesgo regionales, la infraestructura tecnológica y las

²⁸ En el contexto de la seguridad informática, "acceso por puerta trasera" (*backdoor access*) se refiere a un método o vulnerabilidad que permite a un usuario, ya sea autorizado o no, eludir las medidas de seguridad habituales y obtener acceso a un sistema informático, red o aplicación de software.

culturas jurídicas. Por ejemplo, Estados Unidos ha venido adoptando una política proactiva contra el ciberterrorismo centrada en las capacidades cibernéticas ofensivas, la coordinación interinstitucional y la participación global. El Comando Cibernético de los Estados Unidos (USCYBERCOM), en colaboración con la Agencia Nacional de Seguridad (NSA) y el Departamento de Seguridad Nacional, lidera la mitigación y la respuesta ante amenazas ciberterroristas. Operaciones como *Glowing Symphony* que, como ya se mencionó, perturbaron la infraestructura mediática de ISIS, marcaron un cambio estratégico en la estrategia norteamericana de la defensa pasiva a la intervención persistente (Di Pietro et al., 2021).

A nivel nacional, el Departamento de Justicia y el Buró Federal de Investigaciones (FBI) han integrado el ciberterrorismo en los marcos antiterroristas, utilizando la Sección 2339A de la Ley Patriota así como las leyes de ciberdelincuencia para procesar a los facilitadores. La Estrategia Nacional de Ciberseguridad (2023) enfatiza la prevención, la atribución y la fusión cívico-militar, haciendo eco de la visión de Montasari (2023) de una doctrina integrada de inteligencia contra el ciberterrorismo. No obstante, persisten los desafíos, en particular en torno al cifrado, la cooperación con el sector privado y las libertades civiles. Como señaló Vacca (2020), equilibrar la seguridad nacional con las protecciones de la Primera Enmienda continúa alimentando los debates en torno a la vigilancia, la desvinculación de plataformas y la extralimitación de la fiscalía en ese país.

La respuesta del Reino Unido prioriza la resiliencia, la seguridad de la información y la vinculación con la comunidad (Legrand, 2014). El Centro Nacional de Ciberseguridad (NCSC), dependiente del GCHQ²⁹, coordina los esfuerzos nacionales para detectar y disuadir el terrorismo cibernético. Su programa de Ciberdefensa Activa (ACD) bloquea proactivamente los dominios de *phishing* y neutraliza la infraestructura utilizada por los actores de amenazas (Koops, 2016).

Las respuestas legales se basan en la Ley de Terrorismo de 2006, que penaliza la difusión de publicaciones terroristas, incluidos los medios digitales. La Estrategia de Prevención del Reino Unido incluye componentes de contrarradicalización digital, implementando contranarrativas específicas en plataformas frecuentadas por personas en riesgo (Aday, 2019). La colaboración entre académicos y profesionales también es un sello distintivo del modelo británico, ya que las universidades colaboran con las fuerzas del orden para monitorear tendencias y

²⁹ El GCHQ, abreviatura de la "Sede de Comunicaciones del Gobierno", es la agencia de ciberseguridad del Reino Unido. Es una de las tres agencias de Inteligencia y Seguridad del Reino Unido, junto con el MI5 y el Servicio Secreto de Inteligencia (MI6), también conocido como MI6.

capacitar a analistas. Sin embargo, los críticos han señalado el uso excesivo de la vigilancia bajo la Ley de Poderes de Investigación y el riesgo de estigmatizar a las comunidades marginadas.

La política de la OTAN contra el ciberterrorismo está arraigada en su doctrina de defensa colectiva. Si bien los ciberataques por sí solos pueden no activar el artículo 5, las operaciones híbridas que incluyen terrorismo digital se consideran cada vez más amenazas a la seguridad colectiva. El Centro de Excelencia Cooperativa de Ciberdefensa de la OTAN (CCDCOE), en Tallin, lidera la planificación estratégica, la formación de equipos rojos y los juegos de guerra.

Downes y Maglaras (2023) destacan que los marcos de la UE ejemplifican la difusión de normas, ofreciendo instrumentos de derecho indicativo como códigos de conducta para plataformas tecnológicas, y evaluaciones de riesgos para la ciberseguridad del sector público. La Unión Europea ha desarrollado una respuesta multicapa contra el ciberterrorismo a través de su Ley de Ciberseguridad de la UE, el Coordinador Antiterrorista y la Unidad de Referencia de Internet (IRU) de Europol. Estos organismos coordinan la retirada de contenido terrorista y facilitan el intercambio de información entre los Estados miembros de la UE (Wardle & Derakhshan, 2017).

En el Sur Global, las respuestas al ciberterrorismo se ven condicionadas por la limitada capacidad técnica, la dependencia externa y la fragilidad interna. Estados como Nigeria, India y Brasil han avanzado en la cibervigilancia y el desarrollo de los CERT³⁰, pero a menudo carecen de la infraestructura forense y la armonización jurídica necesarias para la cooperación transnacional.

En África, la Convención de la Unión Africana sobre Ciberseguridad (Convención de Malabo), proporciona un marco jurídico regional, pero su ratificación sigue siendo desigual; además, muchos países dependen de la capacitación de la Oficina de las Naciones Unidas contra la Droga y el Delito (UNODC), el apoyo de inteligencia de Interpol y las alianzas con países donantes (Mercado, 2008). La región MENA se enfrenta a desafíos únicos; como observa Gelici (2022), los Estados de la región deben equilibrar la lucha contra el ciberterrorismo con las preocupaciones sobre la censura. Por ejemplo, Egipto y los Emiratos Árabes Unidos han criminalizado ciertos contenidos en línea bajo leyes antiterroristas, desdibujando la línea entre seguridad y represión.

³⁰ Son los Equipos de Respuesta ante Emergencias Informáticas (Computer Emergency Response Team - CERT). Son grupos especializados que se dedican a prevenir, detectar y responder a incidentes de seguridad informática.

Colombia ha desarrollado un marco legal e institucional estructurado para abordar la ciberdelincuencia y la seguridad digital; empero, carece de una definición normativa y una clasificación penal del ciberterrorismo. Esta brecha refleja una tendencia global más amplia: la legislación colombiana tiene dificultades para adaptarse a la evolución de la ciberviolencia con motivaciones políticas. La piedra angular de la regulación colombiana de la ciberdelincuencia es la Ley 1273 de 2009, que reformó el Código Penal (Ley 599 de 2000) para incluir un capítulo sobre delitos contra los datos y sistemas de información y comunicación.

Estas disposiciones tipifican como delito diversos actos como el acceso no autorizado a sistemas informáticos, la interferencia en sistemas, la interceptación y destrucción de datos, la difusión de *malware* y el *phishing*. Si bien estos artículos son esenciales para el enjuiciamiento de los delitos cibernéticos, ninguno define ni sanciona el ciberterrorismo como un delito específico. Este silencio normativo crea un vacío legal para los casos en que las acciones cibernéticas buscan intimidar, coaccionar o generar terror sistémico alineado con objetivos políticos o ideológicos.

Si bien existen amplias leyes de protección de datos, como la Ley 1581 de 2012 y el Decreto 1377 de 2013, que exigen la mitigación de riesgos y la notificación de incidentes, estas leyes se centran en la protección de la privacidad, más que en los imperativos de seguridad nacional. Académicos como Jarvis y Macdonald (2015) han señalado que la falta de claridad en las definiciones a nivel internacional dificulta la armonización de las respuestas. Colombia ejemplifica este desafío a nivel nacional. Las organizaciones terroristas que operan en ámbitos híbridos físico-cibernéticos pueden clasificarse entre las categorías legales de terrorismo común y ciberdelito, lo que puede limitar la capacidad de fiscales y jueces para aplicar sanciones proporcionales y específicas.

A pesar de la ausencia de legislación específica sobre ciberterrorismo, Colombia ha implementado diversas políticas de seguridad digital. El documento CONPES 3701 (2011) sentó las bases de la estrategia nacional de ciberseguridad, haciendo hincapié en la prevención, la coordinación interinstitucional y la protección de la infraestructura. Esto se perfeccionó con el Decreto 338 de 2022, que introdujo requisitos para que los actores públicos y privados que gestionan infraestructuras críticas realicen evaluaciones de riesgos y adopten mecanismos de respuesta a incidentes.

Sin embargo, ninguna de estas políticas aborda ni define explícitamente la prevención del ciberterrorismo. La estrategia de seguridad digital sigue orientada a la

resiliencia económica, la protección de la infraestructura crítica y la gobernanza de datos. Si bien estos esfuerzos demuestran una creciente madurez en la ciber-gobernanza, siguen centrados en el ciberdelito y aún no ofrecen un marco legal o estratégico coherente para amenazas ideológicas como el ciberterrorismo.

El marco actual presenta varias limitaciones. No existe una distinción legal entre el ciberdelito y la violencia digital con motivaciones políticas, lo que dificulta el procesamiento de quienes emplean herramientas cibernéticas con fines terroristas. La legislación en materia de seguridad nacional sigue estando en gran medida desvinculada de la gobernanza digital, lo que genera fragmentación institucional. La integración de la ciberseguridad con los sectores de defensa, inteligencia y antiterrorismo es incipiente, y falta una regulación anticipada sobre amenazas emergentes como el ciberterrorismo potenciado por IA o los ataques financiados con criptomonedas.

Si bien Colombia ha logrado avances sustanciales en infraestructura digital y desarrollo regulatorio, persiste el vacío normativo en torno al ciberterrorismo. Las futuras reformas deben abordar esta brecha conceptual, integrar el ciberterrorismo en la legislación antiterrorista y armonizar la coordinación institucional para garantizar que las respuestas legales, técnicas y estratégicas puedan adaptarse a las amenazas híbridas de la era digital.

Como advierte Montasari (2023), sin una definición unificada, estándares de atribución sólidos y una aplicación transfronteriza eficaz, el ciberterrorismo seguirá siendo un fenómeno legalmente liminal. El desarrollo de tratados internacionales, definiciones armonizadas y capacidades forenses cibernéticas colaborativas es imperativo. Las iniciativas futuras también deben integrar la rendición de cuentas de las plataformas, el derecho a la privacidad y los marcos centrados en las víctimas, garantizando que las iniciativas anticiberterroristas no comprometan los valores democráticos ni repriman la disidencia legítima.

Además, como señala Ariely (2014), la lucha contra el ciberterrorismo exige estrategias adaptativas y multidominio. Mientras que los Estados de altos ingresos se centran en las capacidades ofensivas y los marcos jurídicos, muchos países en desarrollo priorizan el desarrollo de capacidades y la coordinación regional. De cara al futuro, las respuestas estratégicas deben ser inclusivas, interoperables y basadas tanto en el derecho internacional como en la ética digital.

La existencia del Comando Conjunto Cibernético (CCOC) de las Fuerzas Militares de Colombia representa un pilar institucional con gran potencial para enfrentar de manera proactiva las amenazas en el dominio digital, especialmente el

ciberterrorismo. Creado como parte de la modernización doctrinal y tecnológica de las Fuerzas Militares, el CCOC está facultado para ejercer la ciberdefensa y operaciones conducir militares cibernéticas a nivel estratégico, orientadas a proteger la soberanía, los intereses nacionales y la infraestructura crítica en el ciberespacio. Sin embargo, a pesar de sus capacidades técnicas y su mandato estratégico, el papel del CCOC frente al ciberterrorismo aún no ha sido plenamente conceptualizado ni normativamente delimitado dentro del marco más amplio de seguridad nacional. En un entorno donde los actores no estatales (como grupos insurgentes, redes transnacionales o células terroristas ideológicas), pueden emplear herramientas digitales para desestabilizar el orden público, infiltrar sistemas críticos o difundir propaganda violenta, el CCOC está llamado a asumir un papel protagónico en la detección, disuasión y neutralización de operaciones ciberterroristas.

Su contribución debe articularse en tres dimensiones fundamentales. Primero, en el plano operacional, mediante la conducción de operaciones de vigilancia activa, análisis forense y respuesta ofensiva contra infraestructuras utilizadas por actores hostiles, ya sea en el dominio superficial, profundo o clandestino de internet. Segundo, en el plano estratégico, a través de la producción de inteligencia cibernética que anticipa patrones de comportamiento terrorista, identifique alianzas entre cibercriminales e insurgentes, y provea insumos para la toma de decisiones político-militares. Y tercero, en el plano doctrinal y normativo, promoviendo una definición robusta de ciberterrorismo en el derecho colombiano y fortaleciendo los marcos interinstitucionales de cooperación con organismos civiles como el Departamento Nacional de Inteligencia, la Policía Nacional, la Fiscalía, el Ministerio TIC y la Superintendencia de Industria y Comercio.

En tanto organismo con capacidades militares, el CCOC también está en posición de representar al Estado colombiano en ejercicios multinacionales de ciberdefensa, foros doctrinales de la OTAN, y mecanismos hemisféricos de cooperación como los impulsados por la OEA. Este posicionamiento no solo refuerza la postura del país frente a amenazas híbridas y ciberterroristas, sino que contribuye a construir una arquitectura nacional de ciberseguridad con visión integral y capacidad disuasiva efectiva. Por lo tanto, fortalecer el papel del Comando Conjunto Cibernético en la lucha contra el ciberterrorismo no solo es deseable, sino necesario, si se aspira a consolidar una estrategia nacional de ciberseguridad que sea coherente con los desafíos del siglo XXI.

Conclusiones

La exploración académica del hacktivismo y el ciberterrorismo presentada en este capítulo permite articular una serie de conclusiones estructurales y normativas que resultan cruciales para la comprensión contemporánea de los conflictos digitales en la era posmoderna. En primer lugar, se demuestra que el ciberespacio se ha convertido en un teatro de conflicto híbrido, donde convergen la resistencia política, la disidencia simbólica, la guerra de narrativas y la violencia terrorista. A medida que las líneas entre la protesta y el sabotaje, entre el activismo y el crimen, y entre la persuasión y la coerción se difuminan, se vuelve imperativo desarrollar un marco analítico que no reduzca estos fenómenos a categorías binarias, sino que los comprenda como parte de un espectro dinámico de acción política digital.

El análisis histórico y conceptual del hacktivismo evidencia su evolución desde formas tempranas de disrupción simbólica hasta expresiones altamente sofisticadas de insurgencia digital automatizada. Las seis fases delineadas no solamente permiten una periodización teórica del fenómeno, sino que capturan su transformación ontológica y doctrinal, desde el activismo codificado hasta la agencia poshumana alimentada por inteligencia artificial. El hacktivismo, lejos de ser una táctica marginal, se configura como una modalidad emergente de participación política, guerra simbólica y gobernanza algorítmica.

Asimismo, la revisión empírica y teórica del ciberterrorismo demuestra que este no es un fenómeno homogéneo, sino una constelación de amenazas convergentes que incluye propaganda viral, sabotaje técnico, radicalización emocional, financiación anónima y manipulación perceptiva. A través de los estudios de caso sobre ISIS, Hezbolá y las operaciones terroristas facilitadas por Estados, se constata que el ciberterrorismo no solo amenaza las infraestructuras críticas, sino que también erosiona los cimientos de la confianza democrática, capitaliza las vulnerabilidades psicosociales y se adapta de manera continua mediante las herramientas de la Cuarta Revolución Industrial.

En este orden de ideas, no puede ignorarse que la arquitectura algorítmica de las plataformas digitales actúa como un multiplicador inadvertido de propaganda extremista. Los sistemas de recomendación y priorización de contenidos, diseñados para maximizar la retención y la interacción, tienden a favorecer mensajes que generan reacciones emocionales intensas, lo que amplifica narrativas radicales y desinformativas. Esta lógica operativa conecta directamente con las dinámicas de la guerra híbrida y cognitiva, en la medida en que facilita la penetración de marcos

narrativos hostiles en el tejido social y reduce los costos de su diseminación. Comprender el ciberterrorismo, por lo tanto, exige no solo un análisis de capacidades técnicas, sino también una lectura estratégica de la infraestructura global de información que, de manera no intencionada, potencia su alcance y eficacia.

El capítulo también identifica un vacío normativo persistente: la ausencia de una definición jurídica globalmente aceptada del ciberterrorismo. Esta laguna conceptual impide respuestas armónicas, diluye la capacidad punitiva de los Estados y, en algunos casos, habilita la criminalización de la protesta legítima bajo la retórica del antiterrorismo digital. Colombia, pese a sus avances en ciberseguridad y tipificación de delitos informáticos, carece todavía de una doctrina legal precisa para abordar el ciberterrorismo. El papel del CCOC, en este marco, debe trascender la ciberdefensa técnica y proyectarse como un eje de formulación doctrinal, articulación interinstitucional y liderazgo regional en la gobernanza del ciberespacio.

En suma, este capítulo propone que el fenómeno de la violencia digital debe ser comprendido en clave estratégica, simbólica y normativa. La guerra en el ciberespacio no es solamente una lucha por el control de redes o sistemas; es a su vez una disputa por significados, legitimidades y futuros posibles. Ello implica, por un lado, clarificar los umbrales conceptuales entre disidencia digital y violencia digital, incorporando criterios técnicos, semióticos y conductuales que permitan diferenciarlos de forma precisa; por otro, avanzar en el diseño de marcos regulatorios que equilibren la seguridad nacional con la preservación de las libertades civiles, evitando que la urgencia de la protección derive en un exceso punitivo que restrinja derechos fundamentales.

Asimismo, se requiere construir arquitecturas ciberinstitucionales adaptativas, capaces de anticipar, disuadir y responder a amenazas multidimensionales mediante la integración de inteligencia técnica, análisis de narrativas y operaciones de contrainfluencia. A ello debe sumarse el desarrollo de capacidades de resiliencia algorítmica, incluyendo la auditoría sistemática de los sistemas de recomendación y la implementación de estrategias que mitiguen el sesgo de amplificación de contenidos extremistas. Finalmente, resulta esencial impulsar una cooperación internacional más robusta, que permita el intercambio oportuno de inteligencia y la estandarización de procedimientos frente a la radicalización en entornos digitales cerrados y cifrados. Este capítulo, en consecuencia, no solo es una cartografía crítica de las dinámicas de hacktivismo y ciberterrorismo, sino también una invitación a proyectar una imaginación estratégica que trascienda las respuestas reactivas y asuma el ciberespacio como un dominio decisivo en la configuración del poder en el siglo XXI.

En resumen, ciberdisidencia y terrorismo digital son los dos extremos del frente cibercognitivo, ya que uno busca emancipar la conciencia, el otro colonizarla. Mientras la primera expresa una voluntad de resistencia frente al control informacional y la vigilancia algorítmica, el segundo explota las mismas herramientas tecnológicas para implantar narrativas de miedo, odio o dominación simbólica. En ese sentido, ambos fenómenos son productos de una misma ecología digital, donde la infraestructura técnica, los algoritmos y las redes sociales constituyen el nuevo campo de batalla por el control del sentido. Desde la óptica de la guerra cognitiva, la tensión entre emancipación y manipulación no puede resolverse suprimiendo la disidencia, sino comprendiendo su función dentro del equilibrio democrático. En entornos informacionales hiperconectados, toda estrategia de seguridad debe reconocer que la gestión del conocimiento y de la percepción colectiva es tan decisiva como la defensa territorial o cibernética.

El desafío estratégico de las democracias consiste en proteger la libertad cognitiva sin sofocar la disidencia digital que la sostiene. Ello requiere construir una defensa cognitiva institucional capaz de distinguir entre activismo legítimo y manipulación hostil, entre crítica política y desinformación organizada. Tal defensa no se basa en el control de la información, sino en el fortalecimiento del pensamiento crítico, la alfabetización mediática y la resiliencia social frente a la manipulación psicológica. Solo así podrá garantizarse que el ciberespacio siga siendo un ámbito de libertad y no un teatro de dominación mental.

Referencias

- Aday, S. (2019). Virtual violence: understanding the potential power of ISIS' violent videos to buttress strategic narratives and persuade foreign recruits. En C. Bjola, & J. Pamment (eds.), *Countering online propaganda and extremism: The dark side of digital diplomacy* (pp. 140-153). Routledge.
- Akhgar, B., Choraś, M., Brewster, B., Bosco, F., Vermeersch, E., Luda, V., Puchalski, D., & Wells, D. (2016). Consolidated taxonomy and research roadmap for cybercrime and cyberterrorism. En B. Akhgar, & B. Brewster (eds.), *Combatting cybercrime and cyberterrorism: Challenges, trends and priorities* (pp. 295-322). Springer.
- Álvarez, C., Santafé García, J., & Urbano, Ó. (2017). Metamorphosis bellum: ¿mutando a Guerras de Quinta generación? En C. Álvarez (Ed.), *Escenarios y desafíos de la seguridad multidimensional en Colombia* (pp. 145-223). Sello Editorial ESDEG.
- Archer, E. (2014). Crossing the Rubicon: Understanding cyber terrorism in the European context. *The European Legacy*, 19(5), 606-621.
- Ariely, G. (2008). Knowledge management, terrorism, and cyber terrorism. En L. Janczewski, & A. Colarik (eds.), *Cyber warfare and cyber terrorism* (pp. 7-16). Information Science Reference.
- Ariely, G. (2014). Adaptive responses to cyberterrorism. En T. Chen, L. Jarvis, & S. Macdonald (eds.), *Cyberterrorism: Understanding, assessment, and response* (pp. 175-198). Springer.
- Barlow, J. (1996). *A declaration of the independence of cyberspace*. Electronic Frontier Foundation.
- Baudrillard, J. (1994). *Simulacra and simulation*. University of Michigan Press.
- Bennett, W., & Segerberg, A. (2013). *The Logic of Connective Action: Digital Media and the Personalization of Contentious Politics*. Cambridge University Press.
- Besenyő, J., Gulyas, A., & Trifunovic, D. (2023). Hezbollah and the Internet in the Twenty-First Century. *International Journal of Intelligence and CounterIntelligence*, 36(3), 669-685.
- Bjola, C., & Pamment, J. (2019). Introduction: the 'dark side' of digital diplomacy. En C. Bjola, & J. Pamment (eds.), *Countering online propaganda and extremism: The dark side of digital diplomacy* (pp. 1-10). Routledge.
- Burnett, P., & Vescina, V. (2017). *How to do privacy in the 21st century: The true story of hacktivism*. Eyewear Publishing.
- Castells, M. (2009). *Communication power*. Oxford University Press.
- Castells, M. (2012). *Networks of Outrage and Hope: Social Movements in the Internet Age*. Polity.
- Chow, W., & Levin, D. (2025). Muddying the waters: How perceived foreign interference affects public opinion on protest movements. *American Political Science Review*, 119(1), 314-331.

- Coleman, G. (2014). *Hacker, hoaxer, whistleblower, spy: The many faces of Anonymous*. Verso.
- Curran, K., Concannon, K., & McKeever, S. (2008). Cyber terrorism attacks. En L. Janczewski, & A. Colarik (eds.), *Cyber warfare and cyber terrorism* (pp. 1-6). Information Science Reference.
- Dartnell, M. (2006). *Insurgency online: Web activism and global conflict*. University of Toronto Press.
- Deleuze, G., & Guattari, F. (1987). *A thousand plateaus: Capitalism and schizophrenia*. University of Minnesota Press.
- Demertzis, K., Taketzis, D., Skianis, C., Ikiras, P., & Iliadis, L. (2023). Machine learning – based TCP congestion control strategies for cyberterrorism active defense on smart grids. En M. Ferrag, I. Kantzavelou, L. Maglaras, & H. Janicke (eds.), *Hybrid threats, cyberterrorism and cyberwarfare* (pp. 82-108). CRC Press.
- Denning, D. (2000). *Testimony before the Special Oversight Panel on Terrorism*. U.S. House of Representatives.
- Denning, D. (2007). A view of cyberterrorism five years later. *Studies in Conflict & Terrorism*, 28(2), 103-121.
- Di Pietro, R., Raponi, S., Caprolu, M., & Cresci, S. (2021). *New dimensions of information warfare*. Springer.
- Dilipraj, E. (2019). *Cyber Enigma: Unraveling the Terror in the Cyber World*. Routledge.
- Downes, N., & Maglaras, L. (2023). From rules to retribution: the problem of attribution and regulation in the age of cyberwarfare. En M. Ferrag, I. Kantzavelou, L. Maglaras, & H. Janicke (eds.), *Hybrid threats, cyberterrorism and cyberwarfare* (pp. 40-56). CRC Press.
- Drmola, J., Bastl, M., & Mares, M. (2015). Modeling hacktivism using system dynamics. *Journal of Applied Security Research*, 10(2), 238-248.
- Ejazi, F. (2022). Performance of virtual terrorism in cyber space. En E. Ismayil, & E. Karadogan (eds.), *Media and terrorism in the 21st century* (pp. 224-236). IGI Global.
- El Tiempo (2022, 26 de marzo). El dossier de la CIA que prueba nexo entre rusos y disturbios en Bogotá. <https://www.eltiempo.com/unidad-investigativa/la-evidencia-de-los-nexos-de-rusos-con-los-disturbios-en-bogota-660971>
- Farah, D., & Richardson, M. (2022). *Dangerous Alliances: Russia's Strategic Inroads in Latin America*. National Defense University.
- Foucault, M. (1977). *Discipline and punish: The birth of the prison*. Pantheon Books.
- Ganor, B. (2015). *Global Alert: The Rationality of Modern Islamist Terrorism and the Challenge to the Liberal Democratic World*. Columbia University Press.
- Gelici, Z. (2022). Relationship between education, media, and terror. En E. Ismayil, & E. Karadogan (eds.), *Media and terrorism in the 21st century* (pp. 43-63). IGI Global.

- Giansiracusa, N. (2021). *How Algorithms Create and Prevent Fake News*. Apress.
- Gross, M., Canetti, D., & Vashdi, D. (2016). The psychological effects of cyber terrorism. *Bulletin of the Atomic Scientists*, 72(5), 284-291.
- Guarín, M. (2023). *Uso de las estrategias de comunicación en las campañas políticas a través de Twitter y TikTok a la presidencia en Colombia durante el 2022* [Tesis de pregrado]. Fundación Universitaria Los Libertadores.
- Gutiérrez, T. (2024). *Movimientos sociales, campañas de protesta y activismos transnacionales en Centroamérica*. CLACSO.
- Hardy, K., & Williams, G. (2014). What is 'cyberterrorism'? Computer and internet technology in legal definitions of terrorism. En T. Chen, L. Jarvis, & S. Macdonald (eds.), *Cyberterrorism: Understanding, assessment, and response* (pp. 1-24). Springer.
- Jarvis, L., & Macdonald, S. (2015). What is cyberterrorism?. *Terrorism and Political Violence*, 27(4), 657-678.
- Jarvis, L., Nouri, L., & Whiting, A. (2014). Understanding, locating and constructing cyberterrorism. En T. Chen, L. Jarvis, & S. Macdonald (eds.), *Cyberterrorism: Understanding, assessment, and response* (pp. 25-42). Springer.
- Jordan, T. (2002). *Activism!: Direct action, hacktivism and the future of society*. Reaktion Books.
- Jordan, T., & Taylor, P. (2004). *Hacktivism and cyberwars: Rebels with a cause?*. Routledge.
- Karagiannopoulos, V. (2018). *Living with hacktivism: From conflict to symbiosis*. Palgrave Macmillan.
- Karatzogianni, A. (2015). *Firebrand waves of digital activism 1994-2014: The rise and spread of hacktivism and cyberconflict*. Palgrave Macmillan.
- Kearns, A. (2019). The democratisation of hybrid warfare and practical approaches to defeat violent extremism in the digital age. En C. Bjola, & J. Pamment (eds.), *Countering online propaganda and extremism: The dark side of digital diplomacy* (pp. 99-120). Routledge.
- Kijewski, P., Jaroszewski, P., Urbanowicz, J., & Armin, J. (2016). The never-ending game of cyberattack attribution: Exploring the threats, defenses and research gaps. En B. Akhgar, & B. Brewster (eds.), *Combatting cybercrime and cyberterrorism: Challenges, trends and priorities* (pp. 175-192). Springer.
- Koops, B. (2016). Megatrends and grand challenges of cybercrime and cyberterrorism policy and research. En B. Akhgar, & B. Brewster (eds.), *Combatting cybercrime and cyberterrorism: Challenges, trends and priorities* (pp. 3-16). Springer.
- Kramer, F., Starr, S., & Wentz, L. (eds.). (2009). *Cyberpower and national security*. Potomac Books.
- Kruglova, A. (2022). *Terrorist recruitment, propaganda and branding: Selling terror online*. Routledge.

- Lakomy, M. (2021). *Islamic State's online propaganda: A comparative analysis*. Routledge.
- Lasn, K. (1999). *Culture Jam: The Uncooling of America*. HarperCollins.
- Legrand, T. (2014). The citadel and its sentinels: State strategies for contesting cyberterrorism in the UK. En T. Chen, L. Jarvis, & S. Macdonald (eds.), *Cyberterrorism: Understanding, assessment, and response* (pp. 137-154). Springer.
- Leukfeldt, R., & Holt, T. (2020). Social opportunity structures in hacktivism: Exploring on-line and offline social ties and the role of offender convergence settings in hacktivist networks. *Crime, Law and Social Change*, 73, 283-301.
- Lohlker, R. (2022). IS, Internet, and terror. En E. Ismayil, & E. Karadogan (eds.), *Media and terrorism in the 21st century* (pp. 237-253). IGI Global.
- Liotard, J. (1984). *The Postmodern Condition: A Report on Knowledge*. University of Minnesota Press.
- Manor, I., & Crilley, R. (2019). The aesthetics of violent extremist and counter-violent extremist communication. En C. Bjola, & J. Pamment (eds.), *Countering online propaganda and extremism: The dark side of digital diplomacy* (pp. 121-139). Routledge.
- Martens, C., Sharupi, E., & Venegas, C. (2022). El acceso abierto en disputa en América Latina: transformando los medios de comunicación digitales y la tecnología en América Latina. En C. Martens, C. Venegas, & E. Sharupi (eds.), *Activismo digital, medios comunitarios y comunicación sostenible en América Latina* (pp. 15-44). USFQ Press & Universidad del Valle.
- Mercado, S. (2008). International cybercrime convention. En L. Janczewski, & A. Colarik (eds.), *Cyber warfare and cyber terrorism* (pp. 469-476). Information Science Reference.
- Milan, S. (2015). Hacktivism beyond ambiguity: From activism to resistance. *Internet Policy Review*, 4(2), 1-13.
- Moncayo, N. (2022). El ciberactivismo feminista en la Teoría y en la práctica. En C. Martens, C. Venegas, & E. Sharupi (eds.), *Activismo digital, medios comunitarios y comunicación sostenible en América Latina* (pp. 337-362). USFQ Press & Universidad del Valle.
- Montasari, R. (2023). *Countering cyberterrorism: The confluence of artificial intelligence, cyber forensics and digital policing in US and UK national cybersecurity*. Springer.
- Nicholson, J., Keeling, S., & Black, M. (2023). *Countering violent extremism online: Understanding adversity and adaptation in an increasingly complex digital environment*. RAND Corporation.
- Olmedo, R. (2022). Activismo digital: apuntes teórico-conceptuales para una revisión. *Mediaciones*, 29(18), 204-219.
- Pashentsev, E., & Bazarkina, D. (2021). ISIS propaganda on the Internet, and effective counteraction. *Journal of Political Marketing*, 20(1), 17-33.

- Piazza, J., & Guler, A. (2021). The online caliphate: Internet usage and ISIS support in the Arab world. *Terrorism and Political Violence*, 33(6), 1256-1275.
- Raymond, E. (2001). *The cathedral and the bazaar: Musings on Linux and open source by an accidental revolutionary*. O'Reilly Media.
- Romagna, M., & Leukfeldt, R. (2024a). Becoming a hacktivist: Examining the motivations and the processes that prompt an individual to engage in hacktivism. *Journal of Crime and Justice*, 47(4), 511-529.
- Romagna, M., & Leukfeldt, R. (2024b). Social opportunity structures in hacktivism: Exploring online and offline social ties and the role of offender convergence settings in hacktivist networks. *Victims & Offenders*.
- Salatino, M. (2022). Hacia la construcción de estructuras de conocimiento contrahegemónicas. En C. Martens, C. Venegas, & E. Sharupi (eds.), *Activismo digital, medios comunitarios y comunicación sostenible en América Latina* (pp. 149-176). USFQ Press & Universidad del Valle.
- Sampanis, S., Spiliopoulou, M., Kantzavelou, I., & Maglaras, A. (2023). Cyberwarfare in the modern world. En M. Ferrag, I. Kantzavelou, L. Maglaras, & H. Janicke (eds.), *Hybrid threats, cyberterrorism and cyberwarfare* (pp. 1-21). CRC Press.
- Sanabria, L., & Ochoa, H. (2021). *Protesta social digital en Colombia durante el 2021: Nuevas formas de activismo y vigilancia*. Universidad Libre.
- Sauter, M. (2014). *The coming swarm: DDoS actions, hacktivism, and civil disobedience on the internet*. Bloomsbury Academic.
- Schneider, J. (2022). A world without trust: The insidious cyberthreat. *Foreign Affairs*, 101(1), 22-31.
- Tajfel, H., & Turner, J. (1979). An integrative theory of intergroup conflict. En W. Austin, & S. Worchel (eds.), *The social psychology of intergroup relations* (pp. 33-47). Brooks/Cole.
- Téllez, D. (2023). *Emociones en el avispero que marchó por la paz en Colombia: Políticas afectivas, emociones y activismo digital*. Universidad de los Andes.
- Theohary, C., & Rollins, J. (2015). *Cyberwarfare and cyberterrorism: In brief* (CRS Report R43955). Congressional Research Service.
- Vacca, J. (2020). *Online terrorist propaganda, recruitment, and radicalization*. CRC Press.
- von Busch, O., & Palmås, K. (2006). *Abstract hacktivism: The making of a hacker culture*. OpenMute.
- Wardle, C., & Derakhshan, H. (2017). *Information Disorder: Toward an interdisciplinary framework for research and policy making*. Council of Europe.
- Warren, M. (2008). Terrorism and the Internet. En L. Janczewski, & A. Colarik (eds.), *Cyber warfare and cyber terrorism* (pp. 42-50). Information Science Reference.
- Weimann, G. (2005). Cyberterrorism: The sum of all fears?. *Studies in Conflict & Terrorism*, 28(2), 129-149.

- Weimann, G. (2011). Cyber-fatwas and terrorism. *Studies in Conflict & Terrorism*, 34(10), 765-781.
- Wilkinson, P., & Maglaras, L. (2023). Cyberwarfare and cyberterrorism: What is the critical difference?. En M. Ferrag, I. Kantzavelou, L. Maglaras, & H. Janicke (eds.), *Hybrid threats, cyberterrorism and cyberwarfare* (pp. 166-178). CRC Press.
- Wilson, C. (2014). Cyber threats to critical information infrastructure. En T. Chen, L. Jarvis, & S. Macdonald (eds.), *Cyberterrorism: Understanding, assessment, and response* (pp. 123-136). Springer.
- Workman, M., Phelps, D., & Hare, R. (2013). A study of performative hacktivist subcultures and threats to businesses. *Information Security Journal: A Global Perspective*, 22(4), 187-200.
- Zuboff, S. (2019). *The age of surveillance capitalism: The fight for a human future at the new frontier of power*. PublicAffairs.