



Comandos

Retos de las Fuerzas Especiales e Inteligencia en la guerra contemporánea

Luis Alexander Montero Moncada
Óscar Alejandro Garzón Gómez
(Editores)

Colección Seguridad y Defensa

EDITORIAL ESDEG

Comandos

Retos de las Fuerzas Especiales e Inteligencia en la guerra contemporánea



Comandos

Retos de las Fuerzas Especiales e Inteligencia en la guerra contemporánea

LUIS ALEXANDER MONTERO MONCADA

ÓSCAR ALEJANDRO GARZÓN GÓMEZ

(EDITORES)

Escuela Superior de Guerra "General Rafael Reyes Prieto"

Bogotá D.C., 2024

Catalogación en la publicación – Escuela Superior de Guerra “General Rafael Reyes Prieto”

Comandos. Retos de las Fuerzas Especiales e Inteligencia en la guerra contemporánea / editores Luis Alexander Montero Moncada y Óscar Alejandro Garzón Gómez -- Bogotá : Editorial ESDEG, 2024.

309 páginas : ilustraciones, tablas, mapas y gráficos; 24 cm
Incluye referencias bibliográficas al final de cada capítulo

ISBN impreso: 978-628-7602-79-3

E- ISBN: 978-628-7602-80-9

(Colección Seguridad y Defensa)

1. Fuerzas armadas especiales – Colombia 2. Táctica militar -- Colombia 3. Colombia -- Defensa nacional i. Alonso Galindo, Jaime, Brigadier General (prefacio) ii. Montero Moncada, Luis Alexander (editor - autor) iii. Garzón Gómez, Oscar Alejandro, Teniente Coronel (editor - autor) iv. Muñoz, Andrés Acosta, Coronel (autor) v. Serna Osorio, Jorge Eliecer, Mayor (autor) vi. González Martínez, Miguel Antonio (autor) vii. Reyes Pulido, Oscar Leonardo, Mayor (RA) (autor) viii. Cepeda Daza, Helver Orlando, Teniente Coronel (autor) ix. Torres Cabra, Álvaro Iván, Teniente Coronel (autor) x. Lopes da Cunha, Guilherme, (autor) xi. Rodríguez Rodríguez, José Nicolás, Teniente Coronel (autor) xii. Bernal Vallarino, Oscar Mauricio, Teniente Coronel (autor) xiii. Salgado Luzia, Ilmar Ubiratan, Teniente Coronel (autor) xiv. Di Genaro, Ricardo, Mayor (autor) xv. Gutiérrez Oliveros, Jorge Rafael, Teniente Coronel (autor) xvi. Cruz Segura, Juan Guillermo, Teniente Coronel (autor) xvii. Niño Vergara, Humberto Andrés, Teniente Coronel (autor) xviii. Mejía Rosas, Jorge Luis, Coronel (R) (autor) xix. Naranjo Ardila, Jaime Andrés, Teniente Coronel (autor) xx. Albergaria, Fabio (autor) xxi. Ortiz Celis, Pedro Alexis, Teniente Coronel (autor) xxii. Zuleta Juan, David, Teniente Coronel (autor) xxiii. Rubio Ramírez, Oscar Fernando, Teniente Coronel (autor) xxiv. Díaz Jaimes, Jesús María, Teniente Coronel (R) (autor) xv. Colombia. Escuela Superior de Guerra “General Rafael Reyes Prieto”(ESDEG)

UA627.F84C66 2024

Registro Catalográfico SIBFuP 991322015507231

356.160986123

Archivo descargable en formato MARC en: <https://tinyurl.com/esdeg991322015507231>



Comandos: Retos de las Fuerzas Especiales e Inteligencia en la guerra contemporánea

Primera edición, 2024

Editores:

Luis Alexander Montero Moncada

Óscar Alejandro Garzón Gómez

Cubierta:

Raquel Arianne Alvarado Candela con base en imágenes suministradas por Luis Alexander Montero Moncada.

2024 Escuela Superior de Guerra

“General Rafael Reyes Prieto”

Vicedirección de Investigación

Sello Editorial ESDEG

Carrera 11 N°. 102-50 Bogotá D.C., Colombia

www.esdeglibros.edu.co

Colección Seguridad y Defensa

ISBN impreso: 978-628-7602-79-3

ISBN digital: 978-628-7602-80-9

DOI: <https://doi.org/10.25062/9786287602809>

Libro electrónico publicado a través de la plataforma

Open Monograph Press.

Tiraje de 100 ejemplares

Impreso en Colombia

Libro resultado de investigación de la Escuela Superior de Guerra “General Rafael Reyes Prieto”.

El contenido de este libro corresponde exclusivamente al pensamiento de los autores y es de su absoluta responsabilidad. Las posturas y aseveraciones aquí presentadas son resultado de un ejercicio académico e investigativo que no representa necesariamente la posición oficial ni institucional de las instituciones participantes, la Escuela Superior de Guerra “General Rafael Reyes Prieto”, las Fuerzas Militares de Colombia y el Ministerio de Defensa Nacional.



Los libros publicados por el Sello Editorial ESDEG son de acceso abierto bajo una licencia Creative Commons: Reconocimiento-NoComercial-SinObrasDerivadas.

<https://creativecommons.org/licenses/by-nc-nd/4.0/>



Brigadier General
Jaime Alonso Galindo
DIRECTOR

Contralmirante
Omar Yesid Moreno Oliveros
SUBDIRECTOR

Coronel
Aldemar Serrano Cuervo
VICEDIRECTOR DE INVESTIGACIÓN

Coronel
Oscar Otoniel Torres Conde
VICEDIRECTOR ACADÉMICO

Coronel
Verónica Pedraza Martínez
VICEDIRECTORA ADMINISTRATIVA

Capitán de Navío
Ramiro Morales García
VICEDIRECTOR DE PROYECCIÓN INSTITUCIONAL



Coronel
Aldemar Serrano Cuervo
JEFE SELLO EDITORIAL ESDEG

Erika Paola Ramírez Benítez
EDITORA LIBROS ESDEG

Felipe Solano Fitzgerald
CORRECTOR DE ESTILO

Raquel Arianne Alvarado Candela
DIAGRAMADORA

Contenido

Prefacio BG. Jaime Alonso Galindo	09-10
Introducción Luis Alexander Montero Moncada	11-12
Capítulo 1 Fuerzas Especiales en la guerra contemporánea Jorge Serna Luis Alexander Montero Moncada Miguel Antonio González	13-32
Capítulo 2 En la mente del estratega: identificando la estrategia aplicada al sistema de adquisición de blancos Hélver Orlando Cepeda Daza Oscar Leonardo Reyes Pulido	33-64
Capítulo 3 Análisis prospectivo de las Operaciones de Fuerzas Especiales en megaciudades: Colombia y Brasil Álvaro Iván Torres Cabra Guilherme Lopes da Cunha	65-92
Capítulo 4 Amenazas cibernéticas contemporáneas: retos y desafíos para las operaciones especiales en Colombia José Nicolás Rodríguez Rodríguez Oscar Garzón	93-114

Capítulo 5

Operaciones de Fuerzas Especiales frente a sistemas de amenazas basados en guerra política y guerra de información

Oscar Mauricio Bernal Vallarino

Ilmar Ubiratan Salgado Luzia

115-140

Capítulo 6

Guerra especial: de la táctica a la práctica

Jorge Rafael Gutiérrez Oliveros

Luis Alexander Montero Moncada

141-162

Capítulo 7

Soporte ciber a Fuerzas Especiales del Ejército colombiano en ambiente táctico

Juan Guillermo Cruz Segura

Ricardo Di Genaro

163-188

Capítulo 8

Impacto estratégico de las operaciones de desinformación y la respuesta efectiva de las Fuerzas Militares en el siglo XXI

Humberto Andrés Niño Vergara

Miguel Antonio González Martínez

189-208

Capítulo 9

Límites de la inteligencia artificial y la tecnología *big data* en el análisis de Inteligencia

Jaime Andrés Naranjo Ardila

Jorge Luis Mejía Rosas

209-230

Capítulo 10

La geopolítica del crimen organizado en el orden mundial 2.0: un estudio de caso

Pedro Alexis Ortiz Celis

Fabio Albergaria

231-256

Capítulo 11

Operaciones de Inteligencia y guerras en zonas gris

Oscar Fernando Rubio Ramírez

Jesús María Díaz Jaimes

257-286

Capítulo 12

Capacidades ciber en los conflictos contemporáneos

Juan David Zuleta

Andrés Acosta Muñoz

287-310

Prefacio

Brigadier General Jaime Alonso Galindo

Director Escuela Superior de Guerra "General Rafael Reyes Prieto"

La guerra contemporánea ofrece retos nunca antes vistos. Hoy en día, los ejércitos se enfrentan a adversarios mucho más difusos que antes, en entornos propios de zona gris caracterizados por desafíos como el terrorismo, los ciberataques, las operaciones de desinformación o de inestabilidad, el empleo de *proxis*, las acciones de neutralización que emplean sofisticadas herramientas tecnológicas o neurotóxicas y, en general, cualquier medio de ataque no atribuible, pero con altísimo impacto y capacidad de daño. Además, todos estos elementos se suman a un entorno militar convencional donde hay nuevas armas, altamente tecnificadas, que cambian drásticamente la forma de hacer la guerra convencional.

El campo de batalla va más allá de los cinco dominios tradicionales –tierra, mar, aire, espacio y ciberespacio– para incluir el cognitivo, donde una sociedad hiperconectada pone sobre la mesa los mejores ingredientes para desarrollar operaciones de desinformación. En adición, las acciones irregulares en extremo permean estos dominios tradicionales y cambian la forma de conducir las operaciones militares en ellos. El poder de la información basada en el satélite, los vehículos aéreos y navales autónomos capaces de lanzar ataques de enjambre o de manada, proyectiles de uranio empobrecido o misiles hipersónicos, y los sistemas altamente desarrollados de gestión de batalla se unen a los sistemas de armas tradicionales para construir un entorno operacional nunca visto en el pasado.

En este marco, las Operaciones Especiales y la Inteligencia son protagonistas. Estas unidades altamente flexibles, adaptativas, interoperables, invisibles, tecnológicamente poderosas, con altísimas capacidades diferenciales y con la posibilidad de operar tras las líneas enemigas o en los entornos más difíciles, se hacen indispensables para enfrentar y derrotar a los adversarios actuales. No obstante, es necesario repensarlas. Aparentemente, se debe revisar si las capacidades que tienen los ataques de precisión quirúrgica o de guerra especial –capacidades

críticas de las Fuerzas Especiales– se quedan cortas o no para enfrentar estos retos. Asimismo, la Inteligencia debe responder a entornos cada vez más globales, de forma que la inteligencia táctica y operacional se cruza más con la inteligencia estratégica. La calidad, complejidad y rapidez de la información son hoy imperativos irrenunciables si se quiere garantizar el éxito. Pero lo más importante aparece cuando se entiende que en estas guerras de hoy, la Inteligencia y las Fuerzas Especiales deben trabajar en una simbiosis mucho más profunda que la tradicional, casi que borrando la frontera que pueda existir entre ellas.

Allí radica la importancia de este libro. En esta obra, resultado de cuatro años de reflexión académica e investigación del Departamento Ejército de la Escuela Superior de Guerra “General Rafael Reyes Prieto” (ESDEG) sobre doctrina y retos de las Fuerzas Especiales, plantea algunos de los debates más contemporáneos y de mayor impacto sobre el empleo de estas unidades y la Inteligencia en las guerras actuales. Estos aportes son contundentes dada la especificidad del tema y los pocos estudios que hay, desde una perspectiva académica, sobre el universo de las Operaciones Especiales.

Introducción

Luis Alexander Montero Moncada

Editor

El libro *“Comandos. Retos de las Fuerzas Especiales e Inteligencia en la guerra contemporánea”* se presenta como un análisis exhaustivo de los desafíos que enfrentan las Fuerzas Especiales en un mundo en constante evolución. En un contexto global donde la guerra ha adquirido nuevas dimensiones, la obra propone explorar cómo las Fuerzas Especiales deben adaptarse a un entorno militar que no solo es dinámico, sino también influenciado por la tecnología, la conectividad y las doctrinas obsoletas.

Históricamente, las Fuerzas Especiales han sido un componente esencial en la estrategia militar de cualquier nación. Sin embargo, en la actualidad, su relevancia se ha visto amplificada por la aparición de nuevas tecnologías y tácticas de guerra. La guerra moderna no solo se limita al combate convencional, se ha transformado en un campo de batalla multidimensional que incluye ciberataques, drones, inteligencia artificial y operaciones psicológicas. Esta transformación ha creado un entorno donde las Fuerzas Especiales deben operar en condiciones de incertidumbre y complejidad, lo que requiere una revisión profunda de sus doctrinas y estrategias.

Uno de los aspectos más destacados en la discusión del libro es el impacto de las nuevas tecnologías en la guerra. La incorporación de la inteligencia artificial y la automatización en las operaciones militares ha cambiado la forma en que se planifican y ejecutan las misiones. Las Fuerzas Especiales deben aprender a integrar estas tecnologías en sus operaciones, lo que no solo implica un cambio en la formación y capacitación, sino también en la mentalidad de los operadores especiales. La capacidad de adaptarse rápidamente a la tecnología emergente se ha convertido en un imperativo estratégico. Además, las Fuerzas Especiales también enfrentan el desafío de operar en entornos extremadamente cambiantes. La naturaleza de los conflictos actuales, que a menudo son híbridos y asimétricos, requiere que estas unidades sean flexibles y capaces de adaptarse a situaciones imprevistas.

La hiperconectividad de la sociedad moderna presenta retos únicos para las Fuerzas Especiales. Las redes sociales y otras plataformas digitales han cambiado la forma en que se difunde la información y se manipulan las percepciones públicas. En este contexto, las Fuerzas Especiales deben no solo llevar a cabo operaciones encubiertas, sino también gestionar los retos propios de lo informacional y las narrativas. La guerra de la información se ha convertido en un componente crítico de cualquier conflicto, y las Fuerzas Especiales deben estar preparadas para participar en esta nueva dimensión de la guerra.

Aunque el libro se centra en el sistema de Fuerzas Especiales de Colombia, su análisis tiene un valor internacional. Los retos que enfrentan las Fuerzas Especiales en Colombia son representativos de tendencias globales que afectan a todas las naciones. La necesidad de una doctrina actualizada y de un enfoque innovador en la formación y operación es un tema que resuena en el ámbito militar internacional. Este libro se convierte así en un recurso valioso no solo para Colombia, sino para cualquier país que busque entender y adaptarse a las realidades de la guerra contemporánea.

"Comandos. Retos de las Fuerzas Especiales e Inteligencia en la guerra contemporánea" es más que un análisis, es un llamado a la acción para que las Fuerzas Especiales reconsideren sus enfoques y estrategias en un mundo que avanza a un ritmo acelerado. Al abordar los desafíos tecnológicos, operacionales y sociales, el libro proporciona una hoja de ruta para la modernización y adaptación de las Fuerzas Especiales, asegurando que sigan siendo efectivas y relevantes en un panorama de seguridad en constante cambio.

Finalmente, el libro es el resultado del proceso de investigación del Departamento Ejército de la Escuela Superior de Guerra "General Rafael Reyes Prieto", enmarcado en el proyecto *"Naturaleza de la guerra contemporánea. Retos y oportunidades de las Fuerzas Especiales y la inteligencia"*. Este proyecto de investigación contó con el acompañamiento y apoyo del Comando Conjunto de Operaciones Especiales (CCOES) de Colombia, una unidad de élite que reúne a las Fuerzas Especiales de las Fuerzas Militares, así como de la Universidad Conjunta de Operaciones Especiales (JSOU) de Estados Unidos.

Capítulo 1

Fuerzas Especiales en la guerra contemporánea*

DOI: <https://doi.org/10.25062/9786287602809.01>

Jorge Serna

Luis Alexander Montero Moncada

Miguel Antonio González

Escuela Superior de Guerra "General Rafael Reyes Prieto"

Resumen: Las agrupaciones de Fuerzas Especiales son uno de los activos más importantes de un ejército contemporáneo. Esta valoración no se basa solamente en el alto nivel de especialidad y capacidades de combate de estas unidades de élite, sino porque por su naturaleza es el componente más potente y adecuado para enfrentar escenarios de combate asimétricos e híbridos, los más comunes en la guerra contemporánea. En ese sentido, las capacidades de las Fuerzas Especiales colombianas les ofrecen una oportunidad estratégica a la hora de proyectar poder o participar en operaciones de combate con otras agrupaciones e, incluso, como parte de coaliciones internacionales.

Palabras clave: conflicto internacional; defensa; Fuerzas Armadas; guerra; guerra urbana; propaganda.

* Este capítulo es resultado de investigación adscrito al proyecto "*Naturaleza de la guerra contemporánea. Retos y oportunidades de las Fuerzas Especiales y la Inteligencia*", adscrito al Departamento Ejército de la Escuela Superior de Guerra, inscrito en la línea de investigación "Naturaleza de la guerra, terrorismo, nuevas amenazas", que forma parte del grupo de investigación Centro de Gravedad, categorizado en A, con código COL0104976. Se presenta como opción de grado elaborado por el Mayor Jorge Serna, en la Maestría de Seguridad y Defensa Nacionales de la Escuela Superior de Guerra "General Rafael Reyes Prieto". Los puntos de vista pertenecen a los autores y no reflejan necesariamente los de las instituciones participantes.

Jorge Serna

Mayor del Ejército Nacional de Colombia. Magíster en Seguridad y Defensa Nacionales, Escuela Superior de Guerra “General Rafael Reyes Prieto”, Colombia. Profesional en Ciencias Militares, Escuela Militar de Cadetes “General José María Córdova”, Colombia.

Contacto: jorge.sernaos@buzonejercito.mil.co

Luis Alexander Montero Moncada

Doctorando en Estudios Políticos, Universidad Externado de Colombia, y en Estudios Políticos y Relaciones Internacionales, Universidad Nacional de Colombia. Magíster (*honoris causa*) en Inteligencia Estratégica, Escuela de Inteligencia “Brigadier General Ricardo Charry Solano”, y en Análisis de Problemas Políticos, Económicos e Internacionales Contemporáneos, Instituto de Estudios Políticos de París Sciences-Po, Universidad Externado de Colombia y Ministerio de Relaciones Exteriores de Colombia. Politólogo con énfasis en Relaciones Internacionales, Universidad Nacional de Colombia.

<https://orcid.org/0000-0003-3420-0863> - Contacto: luis.montero@esdeg.edu.co

Miguel Antonio González

Doctorando en Estudios Estratégicos, Seguridad y Defensa, Escuela Superior de Guerra “General Rafael Reyes Prieto”, Colombia. Magíster en Historia, Universidad Nacional de Colombia. Profesional en Relaciones Internacionales y Estudios Políticos, Universidad Militar Nueva Granada, Colombia. Docente e investigador, Departamento Ejército, Escuela Superior de Guerra “General Rafael Reyes Prieto”, y docente del Programa de Relaciones Internacionales y Estudios Políticos FAEDIS, Universidad Militar Nueva Granada, Colombia..

<https://orcid.org/0000-0002-6034-912X> - Contacto: miguel.gonzalez@esdeg.edu.co

Citación APA: Serna, J., Montero Moncada, L. A., & González, M. A. (2024). Fuerzas Especiales en la guerra contemporánea. En L. A. Montero Moncada & O. A. Garzón Gómez (Eds.), *Comandos: Retos de las Fuerzas Especiales e Inteligencia en la guerra contemporánea* (pp. 13-32). Sello Editorial ESDEG. <https://doi.org/10.25062/9786287602809.01>

COMANDOS: RETOS DE LAS FUERZAS ESPECIALES E INTELIGENCIA EN LA GUERRA CONTEMPORÁNEA

ISBN impreso: 978-628-7602-79-3

ISBN digital: 978-628-7602-80-9

DOI: <https://doi.org/10.25062/9786287602809>

Colección Seguridad y Defensa

Sello Editorial ESDEG

Escuela Superior de Guerra “General Rafael Reyes Prieto”

Bogotá D.C., Colombia

2024



Introducción

La naturaleza cambiante de la guerra se ha convertido en un tema recurrente en los estudios militares. Desde los autores clásicos, como Carl von Clausewitz, hasta los contemporáneos, como Kaldor (2001) y Münkler (2002), los investigadores han dirigido sus esfuerzos a estudiar las mutaciones de los conflictos y los factores – exógenos y endógenos– que intervienen en este proceso. Desde una perspectiva analítica cronológica, hay un consenso en que la Guerra Fría constituye un hito de aceleración de los cambios hacia las *nuevas guerras*, pues desde este período se acentúan fenómenos como la reducción de las guerras interestatales en favor del incremento de las guerras irregulares patrocinadas por actores no estatales, los “señores de la guerra”, y, por esta vía, la asimetría de la acción bélica.

La privatización de la violencia bélica en manos de actores no-estatales (Münkler, 2002) supone nuevos retos para las Fuerzas Militares porque cambia el teatro de las operaciones de la guerra. La guerra irregular difumina los clásicos frentes de lucha, elimina las grandes batallas en favor de acciones aisladas y borra la frontera entre lo táctico y lo estratégico. En este sentido, el presente capítulo tiene como norte analizar el papel de las Fuerzas Especiales (FF. EE.) en escenarios híbridos y asimétricos, así como, puntualmente, en las *nuevas guerras*. La hipótesis de trabajo consiste en afirmar que, por su naturaleza flexible, móvil, adaptativa, autosostenible y con altas capacidades de impactar estratégicamente en una campaña, las FF. EE. son la herramienta más efectiva e idónea para contrarrestar las amenazas emergentes producto de esta nueva realidad.

Las FF. EE. son unidades conformadas por el personal más selecto, con un exigente entrenamiento y, por lo mismo, constituyen la élite militar. Son el activo estratégico más importante de los Estados contemporáneos porque sus resultados operacionales superan con creces la inversión en cada unidad. Por lo general, las

FF. EE. operan en grupos pequeños, lo que les permite maniobrar de manera sostenida, ágil y versátil en el teatro de operaciones. Adicionalmente, por su estricto entrenamiento en diversas áreas (combate cuerpo a cuerpo, paracaidismo, buceo, telecomunicaciones, supervivencia en diversas condiciones, manejo de distintas armas, entre otras), resultan claves en el apoyo a las misiones en las guerras convencionales y protagonistas en las guerras asimétricas e híbridas.

Para desplegar esta línea argumental, el capítulo se divide en tres secciones. En la primera, titulada “Caracterización de los escenarios de guerra asimétrica y guerra híbrida en el sistema internacional contemporáneo”, se describe el nuevo escenario global como un efecto de la evolución histórica del arte de la guerra y se identifican los elementos asimétricos e híbridos en los que se enfocan las FF. EE. De hecho, las *nuevas guerras* se desarrollan en un ambiente cada vez más volátil, incierto, complejo y ambiguo (VICA), y allí deben operar las agrupaciones especiales.

La segunda sección, “Elementos doctrinales que hacen idóneo el empleo de las Fuerzas Especiales en la guerra asimétrica y la guerra híbrida”, tiene como propósito, a partir de la doctrina, definir las capacidades de combate que destacan a las FF. EE. Así, se resalta su interoperabilidad, el mando tipo misión y el estricto entrenamiento que reciben las unidades. Una vez se ha estudiado el marco de las guerras contemporáneas y los elementos característicos que distinguen a las FF. EE., la última sección, “El empleo de las Fuerzas Especiales en escenarios de guerra asimétrica y guerra híbrida”, establece algunos ejemplos de cómo se han usado las Operaciones Especiales en los conflictos contemporáneos.

Caracterización de los escenarios de guerra asimétrica y guerra híbrida en el sistema internacional contemporáneo

En el campo de estudios de la seguridad y la defensa, y de forma particular en los estudios militares, subyace una rica literatura dedicada a interpretar el fenómeno de la guerra. En el plano contemporáneo despunta la ya clásica propuesta de William Lind (2005) sobre las *cuatro generaciones de las guerras*: la línea evolutiva inicia con las guerras de primera generación, marcadas por la consolidación de la idea de Estado, la organización inflexible en ejércitos y la búsqueda de la batalla decisiva. Las de segunda generación, por su parte, se caracterizan por los efectos

que tuvo la “era de las revoluciones”, en la cual si bien se mantuvieron la inflexibilidad en la maniobra y la acción de frentes de batalla con amplísimos ejércitos, también se introdujeron nuevos conceptos y doctrinas. Las guerras de tercera generación implicaron una concepción completamente nueva, basada en principios de flexibilidad, maniobra, elasticidad, velocidad y una nueva dimensión del mando tipo misión, que permitía el empleo de grupos y cuerpos de ejércitos, de manera que era a la vez ágil y dinámica. Al respecto, Aznar Montecinos (2015) complementa la discusión sobre la guerra de esta generación afirmando que “se fundamentan en la tecnología”, mientras que “el factor que coadyuva a la definición de las de cuarta es la globalización y el retorno al hombre” (p. 7).

Así las cosas, del aporte de Lind (2005) se desprenden nuevos conceptos sobre la naturaleza de la guerra, que se conjugaron con los conflictos de posguerra mundial matizados por la bipolaridad. De esa manera, la polemología entró en la discusión de las formas ideales para comprender y enfrentar las guerras que no implicaran el encuentro de grandes ejércitos.

El concepto de la *guerra irregular*, por tanto, está vinculado con la *guerra popular prolongada*, acuñado doctrinariamente por el líder de la Revolución China, Mao Tse Tung, quien formuló el paso de la guerra de guerrillas a la de movimientos y posteriormente a la guerra de posiciones a través de esta estrategia prolongada para conquistar el poder.

De hecho, Mao ya destacaba la movilidad como un factor esencial en la guerra de guerrillas, de manera que incluso su respuesta –la doctrina de la contrainsurgencia y posteriormente la del conflicto de baja intensidad– debería propender al mismo elemento. Al respecto, Mao Tse Tung (1967) consideraba:

La cuestión de la iniciativa [y de la flexibilidad de las fuerzas irregulares] es aún más vital en la guerra de guerrillas. Porque las unidades guerrilleras en su mayoría operan en circunstancias muy difíciles: combaten sin retaguardia, se enfrentan con sus débiles fuerzas a las poderosas fuerzas del enemigo, no poseen suficiente experiencia (cuando se trata de unidades guerrilleras recién organizadas), están aisladas unas de otras, etc. No obstante, la iniciativa en la guerra de guerrillas puede obtenerse, con la condición esencial de que aprovechemos las tres debilidades antes mencionadas del enemigo. Aprovechando la insuficiencia en efectivos de las fuerzas enemigas, las unidades guerrilleras pueden utilizar audazmente vastas zonas como terreno de operaciones. (p. 175)

Este asunto también se ha discutido desde otras perspectivas. Por ejemplo, para Miron (2019), las guerras irregulares, como escenario operacional novedoso y difundido, implica un carácter diferencial sustancial con las guerras convencionales:

[...] a diferencia de las guerras convencionales, se refieren principalmente al *modus operandi* empleado por uno o todos los beligerantes. Con frecuencia, este *modus operandi* es favorecido por el lado más débil y consiste en ataques sorpresa, tácticas de guerrilla y terrorismo, para alcanzar un objetivo político. A menudo, se les atribuye a actores no estatales que no tienen el monopolio del uso legítimo de la fuerza física. (p. 459)

Aunque este concepto se asocia a las guerrillas que surgieron en el contexto de la Guerra Fría, en algunos casos su vigencia teórica sobrepasó los años sesenta y aún se constata en la actualidad, como sucede en Colombia. Cuando terminó la Guerra Fría, la comprensión de la naturaleza de la guerra tuvo que encaminarse al estudio de lo que Lind (2005) definió como las *guerras de cuarta generación*, en las cuales se conservan

[...] la descentralización e iniciativa [...], pero en otros aspectos la cuarta generación señala el cambio más radical desde la Paz de Westfalia. En la guerra de cuarta generación, el Estado pierde su monopolio de la guerra. Alrededor del mundo, las FF. AA. se hallan hoy luchando en contra de oponentes no estatales tales como al-Qaeda, Hamas, Hezbolá y las FARC. En casi todos los lugares, el Estado está perdiendo. (p. 15)

El autor ofrece, por tanto, un marco analítico para perfilar los nuevos conflictos de post Guerra Fría, mucho más irregulares, amorfos y que involucran un alto número de protagonistas no estatales. Lind (2005) profundiza en las características de estas confrontaciones y propone que

[...] la guerra de cuarta generación también está caracterizada por un retorno al mundo de culturas, y no simplemente Estados en conflicto. En la guerra de cuarta generación, la invasión mediante la inmigración puede ser tan peligrosa como la invasión que emplea un ejército de Estado. (p. 14)

En este sentido, la guerra asimétrica se entiende como un conjunto de prácticas operacionales que tienen por objeto negar las ventajas y explotar las vulnerabilidades de la parte más fuerte, antes que buscar enfrentamientos directos (Herman, 1997). Esta perspectiva, sin embargo, es debatida por autores como Cabrerizo

(2002) y el mismo Lind (2005), toda vez que la asimetría no puede limitarse a una disparidad en el poder de fuego que marque un desenfoque operacional, sino que, por el contrario, va mucho más allá e incorpora aspectos extremadamente irregulares en el componente armado, los cuales son apoyados por factores psicológicos, sociales e incluso comunicacionales. Este error elemental de enfoque afecta también visiones como la de Verstrynge (2005), quien reduce drásticamente lo asimétrico a la disparidad de fuerza. Para el autor, “los conflictos asimétricos no son otra cosa que un enfrentamiento entre fuerzas de distinta capacidad y tamaño, y como tal recurren a estrategias diferentes, que en el caso del más débil se escapan a los métodos convencionales” (Verstrynge, 2005, p. 72).

No obstante, Verstrynge (2005) acierta en la caracterización específica que hace de la guerra asimétrica, la cual permite entender que se empleen las FF. EE. como respuesta estatal a este tipo de adversario. De hecho, los postulados de Verstrynge (2005) implican una respuesta flexible, totalmente ágil, autosostenible, casi que invisible y con un muy alto poder combativo, sin necesidad de que las acciones se basen en formaciones tradicionales, pesadas y poco móviles. De acuerdo con Verstrynge (2005), las características de un adversario asimétrico son las siguientes:

- a. El empleo de técnicas diferentes a las convencionales y poco efectivas.
- b. Una base no nacional o transnacional, lo cual hace difícil su identificación y localización.
- c. La libertad de escogencia del terreno o del área de operaciones para dificultar que el adversario aplique su mayor poder.
- d. El predominio de la sorpresa.
- e. Privilegiar acciones irregulares que impliquen un muy bajo coste en comparación con el efecto estratégico que se pueda alcanzar.
- f. Contar con un mando centralizado que se complemente con unidades operativas descentralizadas y autónomas, lo cual le permite flexibilidad operacional y sensación de copamiento.
- g. No estar obligado por el derecho de la guerra ni por el Derecho Internacional Humanitario (DIH).
- h. Enfatizar en ataques físicos que minen la credibilidad de los Estados.
- i. Involucrar al máximo a la población civil.
- j. Diseñar operaciones de manera que tengan la máxima visibilidad y alcance mediático.
- k. Prolongar las acciones lo máximo posible en el tiempo para desgastar al adversario más fuerte.

Evidentemente, este recetario sugiere que una unidad militar convencional no puede enfrentar con éxito a un adversario asimétrico, por lo cual se requiere una unidad mucho más flexible y decisiva. Precisamente, estas son las agrupaciones de FF. EE.

Este enfoque es profundizado por Metz y Johnson (2001), quienes enfatizan que es necesario flexibilizar el poder militar de una operación en función del éxito. Evidentemente, las experiencias operacionales de Estados Unidos, en especial las que desplegó en Irak y Afganistán, ilustran esta perspectiva, sobre todo si se tiene en cuenta la manera como Metz y Johnson (2001) caracterizan al adversario asimétrico:

Acting, organizing, and thinking differently than opponents in order to maximize one's own advantages, exploit an opponents' weaknesses, attain the initiative or gain greater freedom of action. It can be political –strategic, military– strategic, operational or a combination of these. It can entail different methods, technologies, values, organizations, time perspectives or some combination of these. (p. 24)

En el plano local, Sánchez et al. (2012) coinciden en la condición de interoperabilidad, flexibilidad y sostenibilidad de las tropas comprometidas en una confrontación asimétrica. Para los autores, es imprescindible que los Estados tengan en cuenta factores como las plataformas de supervivencia para el combate y una resistencia dinámica que permita la movilidad y la sostenibilidad (Sánchez et al., 2012).

Más allá de las ciencias militares y llevando la discusión hacia las relaciones internacionales, para el análisis propuesto en este capítulo resultan fundamentales dos concepciones ligadas con los estudios contemporáneos de la guerra en el marco que Münkler (2002) y Kaldor (2001) catalogan como *nuevas guerras*. Aunque algo etérea, esta definición plantea que hay una transición en la cual los Estados dejan de ser los actores monopolizadores del recurso de la guerra –que ostentaban desde la configuración de las relaciones internacionales contemporáneas a partir del pacto de Westfalia en el siglo XVII–, para ceder parcialmente esta capacidad a actores privados, subnacionales o incluso tribales.

La asimetría, que hace referencia a la disparidad de los combatientes, se explica en el hecho de que los costos de la guerra se reducen y en consecuencia las armas se pueden conseguir con relativa facilidad. De esta manera, pequeños grupos insurgentes tuvieron la capacidad de adquirir armamento proveniente del mercado negro con cierta facilidad y rapidez. Además, en la medida en que se anula el combate convencional, los combatientes se dirigen a otros blancos más débiles, como la población civil (Münkler, 2002, p. 4).

Aunque bastante menos precisas que en las ciencias militares, las definiciones de Münkler (2002) y Kaldor (2001) dejan ver también que para enfrentar estos retos se requieren unas fuerzas diferentes a las tradicionales, mucho más cercanas a las capacidades que ofrecen las FF. EE. Esta condición se agudiza cuando los actores involucrados en la guerra asimétrica la complementan con medios convencionales para proponer escenarios mucho más retadores. Esta conjunción implica la aparición de un nuevo concepto: la *guerra híbrida*.

Desde las primeras aproximaciones a esta noción, se ha propuesto que lo *híbrido* se refiere al empleo de las capacidades convencionales junto con el despliegue de la guerra especial y las unidades de las FF. EE. Por ello, Robert G. Walker (1998) recurría al *Fleet Marine Force Manual Warfighting FMFM-7* para enfatizar que “las guerras del siglo XXI se caracterizarán por una mezcla íntima de acciones convencionales y especiales” (p. 36).

Por su parte, Hoffman (2009), precursor del concepto, definió la guerra híbrida como

[...] una amenaza que, susceptible de ser utilizada tanto por Estados como por actores no-estatales, aprovecha toda la gama de modos y estilos de lucha disponibles. Estos pueden incluir formas convencionales; tácticas y orgánicas irregulares, actos terroristas fundamentados en el uso de la violencia y la coerción de forma indiscriminada; e incluso actos criminales. (p. 35)

La perspectiva de Hoffman (2009) es visionaria porque abre el camino para que se conciba emplear las FF. EE. en escenarios combinados de guerra convencional y asimétrica. Desde su perspectiva, estas unidades están más vigentes que en cualquier otro momento, idea que se reafirmó en la guerra de 2006 entre Hezbolá e Israel, donde el planteamiento de la milicia chiita mostró la efectividad que puede tener mezclar acciones flexibles y convencionales.

Posteriormente, Guillem Colom (2012) recogió y refinó el pensamiento de Hoffman, así como el de Wilkie y Lasica, para caracterizar la guerra híbrida como

[...] la plena integración en tiempo y espacio de procedimientos típicamente convencionales con tácticas propias de la guerra irregular (desde las clásicas emboscadas o acciones de propaganda, agitación e insurgencia, hasta actividades de guerra informativa, guerra legal o ciberguerra), mezcladas estas últimas con actos terroristas y conexiones con el crimen organizado para la obtención de apoyos y asistencia de todo tipo. (Colom, 2012, p. 80)

Acá el rasgo distintivo del empleo de las FF. EE. también sale a flote, pues es el medio más eficaz y potente para contrarrestar la acción de guerra irregular. El historiador toma uno de los elementos analíticos de Hoffman (2009) y recurre al elemento histórico para evaluar el carácter novedoso de lo híbrido. También en ese sentido, Thomas Huber (1996)

[...] describe el fenómeno de las fuerzas regulares e irregulares que combaten de manera coordinada. Huber explica la guerra compuesta a modo de marco intelectual para entender el fenómeno de las fuerzas convencionales (regulares) y las fuerzas no convencionales (irregulares) que operan bajo dirección unificada a fin de lograr el estado final deseado. (García et al., 2015, p. 3)

Aunque aparentemente hay una recurrencia histórica a combinar las acciones convencionales con las irregulares, esto no es suficiente para proponer que la guerra híbrida ya haya sido empleada y que sea usual. Por el contrario, los requerimientos contemporáneos del combate asimétrico implican que sus características híbridas obligan a recurrir a las FF. EE.

Una vez establecidos los ejes teóricos-conceptuales que guían el presente capítulo, es posible afirmar que, claramente, los flujos de interacciones y de cambios cada vez más vertiginosos en el sistema internacional inciden profundamente en la naturaleza de la formulación teórica que se hace sobre las guerras contemporáneas. La mutación de las amenazas y su complejidad dificultan que la comunidad experta las defina con precisión, lo cual tiene un impacto en el concepto mismo de seguridad internacional y en las formas de hacer la guerra.

En el campo práctico, el pensamiento estratégico de algunos líderes políticos permite que surjan medidas para contrarrestar las amenazas que vulneran la soberanía o el orden político interno, sin embargo esto puede crear tensiones domésticas e internacionales. Un caso concreto se puede situar en los denominados *rogue states*: Cuba, Irán, Nicaragua, Corea del Norte, Siria y Venezuela. Una lectura crítica a esta denominación se encuentra en Chomsky (2000), quien afirma que los gobernantes mantienen un amplio número de estrategias para cumplir sus objetivos o intereses, que por lo general redundan en el sostenimiento de sus regímenes. La ubicación geopolítica de los *rogue states* permite una distribución homogénea de focos de tensión dentro del escenario internacional actual, los cuales, sumados a las tensiones internas –clásicas en países en vía de desarrollo– que son alimentadas por algunos sectores, provocan caos e inestabilidad. La presencia de economías ilegales derivadas del narcotráfico, la minería ilegal, el tráfico de armas

y la trata de personas, entre muchos otros factores, aumentan el efecto desestabilizador en el Estado, toda vez que adquieren importantes recursos para realizar acciones terroristas.

Asimismo, la globalización se ha profundizado en el sistema internacional contemporáneo, lo cual ha permitido que surjan nuevas alianzas dentro de un orden internacional difuso y complejo en el que asoman nuevos liderazgos alternativos al poder de Estados Unidos desde el fin de la Guerra Fría. De esta manera, el mundo transita hacia un orden multipolar en el cual el protagonismo emergente de China –y en alguna medida Rusia– devela la posibilidad de que se presente un nuevo teatro de confrontación a gran escala, en el cual se combinan nuevas modalidades de hostilidades, como las digitales. Todo esto es, nuevamente, el escenario idóneo para las FF. EE.

Elementos doctrinales que hacen idóneo emplear las Fuerzas Especiales en la guerra asimétrica y la guerra híbrida

Las FF. EE. o Cuerpos de Élite forman unidades militares con base en un entrenamiento especializado y se caracterizan por ser muy ágiles y versátiles en el desarrollo de las operaciones asignadas. Llevan a cabo una serie de tareas específicas y se encargan de labores para las cuales han recibido un entrenamiento más duro, mecánico, fuerte y riguroso que las tropas regulares. Contrario a las unidades convencionales, las FF. EE. utilizan un equipamiento más avanzado que les asegura un máximo poder de fuego y obtienen una información más amplia, clara y puntual de sus objetivos.

Se trata de unidades ágiles y versátiles que tienen una formación más amplia y medios con más tecnología que las demás fuerzas. Una unidad de FF. EE. está entrenada para llevar a cabo misiones de combate cercano de forma directa o indirecta, de sabotaje, infiltración, inteligencia y reconocimiento especial. Por lo tanto, se puede proponer que las unidades de FF. EE. son la mejor alternativa que disponen las Fuerzas Militares para enfrentar, con la más elevada probabilidad de éxito, las amenazas asimétricas o híbridas que atentan de manera globalizada contra la seguridad de los Estados.

Por su naturaleza, las FF. EE. son agrupaciones diseñadas para hacer contactos tácticos decisivos de alcance estratégico y salir victoriosas, en la medida

en que infiltran en lo profundo del adversario o en una zona muy dinámica, sin la posibilidad de apoyo de fuegos o de otras unidades convencionales durante la operación. Requieren la máxima sorpresa, agilidad, flexibilidad organizacional y de maniobra, así como ser autosuficientes en logística y en poder.

Las FF. EE. deben ser consideradas como los activos de alto valor estratégico para los Estados, pues su entrenamiento les permite ejecutar misiones de gran importancia para la supervivencia del Estado, en las cuales entremezclan la táctica y la estrategia: desde operaciones de acciones ofensivas hasta actuaciones de reconocimiento reservado para la obtención de información. Además, pueden realizar sus operaciones de forma independiente o conjunta con fuerzas convencionales y con otras organizaciones del Estado. Suponen además el empleo de recursos mínimos, en la medida en que son unidades pequeñas con misiones concretas que pueden afectar de forma contundente a rivales militares superiores con eficacia y precisión quirúrgica. En otras palabras, las Operaciones Especiales son realizadas en apoyo a un teatro específico de operaciones o contra objetivos estratégicos u objetivos de alto valor. Como advierte Sigüeñas (2018),

[...] la mayoría de las operaciones especiales son diseñadas para mejorar las probabilidades de éxito de la campaña militar en una zona de operaciones o de guerra. Así mismo, estas operaciones multidisciplinarias o conjuntas, aunque pueden ser conducidas como operaciones independientes, se planifican y se llevan a cabo como operaciones conjuntas dado el requerimiento de múltiples especialidades precisas rutinariamente, para el soporte y la coordinación de la operación. (p. 56)

Por sus características elementales, las FF. EE. cumplen tareas fundamentalmente dirigidas a las nuevas guerras. Tanto en la guerra asimétrica como en la guerra híbrida, las FF. EE. proyectan sus capacidades en escenarios de confrontación no convencionales porque su flexibilidad e interoperabilidad son idóneas para enfrentar enemigos igual de flexibles y difusos, como los que predominan en estas guerras.

Además, el entrenamiento y las capacidades que tienen las FF. EE. en materia de lucha contra el terrorismo, de inteligencia y de espionaje en teatros de operación hostiles previenen actos delincuenciales, como atentados a gran escala, cuyos blancos buscan impactar en la población civil. En consecuencia, sus destrezas y capacidades especiales no deben ser usadas en tareas ni en misiones que las desgasten, pues estas acciones las pueden realizar las tropas convencionales. Al respecto, Trejo (2018) señala que,

[...] en la actualidad, las Fuerzas Especiales –además de su capacitación específica en operaciones convencionales–, se especializaron en la lucha contra el terrorismo, que constituye la principal amenaza de los países desarrollados. Estas fuerzas demostraron flexibilidad y capacidad de adaptación, pero sobre todo ingenio y creatividad con el cumplimiento de las misiones impuestas. (p. 49)

Las operaciones especiales tienen por esencia una implicación estratégica u operacional. Por ello, el planeamiento operacional parte de conocimientos concretos del objetivo para explotarlas mejor, toda vez que el esfuerzo se enfoca totalmente en ataques rápidos y certeros, separando las demás agrupaciones que corresponden a una guerra convencional. En otras palabras, las tareas se deben desarrollar empleando tácticas, técnicas y procedimientos para planear, preparar y ejecutar operaciones especiales en todo momento y lugar, de manera autónoma y autosostenible.

En el entorno de la doctrina de las operaciones militares se señala que las Operaciones Especiales son conducidas en ambientes hostiles, negados o sensibles, con el propósito de conseguir objetivos militares, políticos, económicos, diplomáticos y/o informativos. Además, estas acciones emplean capacidades militares que no demandan la acción de las fuerzas convencionales y requieren total discreción, clandestinidad y poca visibilidad al protagonismo. Así las cosas, es posible afirmar que las FF. EE. son el componente asimétrico dentro de una fuerza estatal.

Este enfoque ha implicado un cambio profundo y constante en la doctrina y en la estructura de las Fuerzas Militares, toda vez que pretende adecuar este potencial de fuerza a los nuevos escenarios asimétricos e híbridos. Con este propósito, estas tropas especiales reciben un entrenamiento idóneo para enfrentar amenazas domésticas, subnacionales, tribales, ideológicas, terroristas, irregulares, de milicias, convergentes, internacionales o transnacionales.

Tanto la guerra asimétrica como la guerra híbrida están en constante evolución, de manera que las unidades de Operaciones Especiales deben mantener a la par su avance para contrarrestar todo acto hostil o impedir que se realice. Por esta razón, el enfoque y el trabajo de una agrupación de FF. EE. debe ser totalmente proactivo para que ajuste continuamente sus capacidades, doctrina, equipo y poder relativo a las mutaciones que ofrezcan los adversarios asimétricos e híbridos.

En ese sentido, el terrorismo, por ejemplo, cuenta la mayoría de las veces con la sorpresa como factor determinante para cometer la acción violenta. Los Estados tratan de contrarrestar dichos actos con la Inteligencia especializada y dominante frente a cada una de sus amenazas, ya sea interna o externa, pero es mediante la acción directa de las agrupaciones de FF. EE. que pueden abatir blancos estratégicos para desarticular organizaciones altamente mimetizables.

Por consiguiente, los Estados deben aplicar los elementos doctrinales necesarios para enfrentar las amenazas emergentes, entre los cuales tienen un lugar especial las FF. EE. Por su parte, el contexto de las fuerzas multilaterales evidencia un entrenamiento más amplio, ya que estas deben evaluar las fuerzas enemigas que pueden llegar a confrontar y eso hace que incrementen sus capacidades de combate.

Queda claro, entonces, que las FF. EE. cobran suma preponderancia para las Fuerzas Militares, así como para el desarrollo de operaciones no convencionales por tierra, mar o aire, e incluso en escenarios de ciberguerra, durante los conflictos internos o externos de las naciones. Estas actividades incluyen incursiones ofensivas, demoliciones, reconocimiento, contraterrorismo y búsqueda y rescate. Como se mencionó, además de su entrenamiento riguroso constante, los miembros de las FF. EE. suelen tener capacidades especializadas en nado, buceo, paracaidismo, supervivencia, medicina de emergencia e idiomas extranjeros.

Las capacidades de estas unidades deben mejorar diariamente para responder a la incesante evolución de la guerra contemporánea, de manera que es posible afirmar que hacen la diferencia en los ambientes de las nuevas guerras. Históricamente, la doctrina de las FF. EE. implica características como:

- Mantener la calma en situaciones de máxima tensión.
- Trabajar como integrante de un equipo altamente especializado.
- Tener plena predisposición para enfrentar desafíos muy exigentes.
- Enfrentar el mayor peligro posible sin posibilidad de apoyo inmediato y con recursos limitados.

En el plano regional, luego de la Segunda Guerra Mundial y como parte de los acuerdos del Tratado Interamericano de Asistencia Recíproca, las Fuerzas Armadas latinoamericanas realizaron una serie de modificaciones a sus estructuras orgánicas y a su doctrina con el propósito de crear Fuerzas de Operaciones Especiales que se ajustaran a los desafíos que demandaba el escenario de posguerra. En la actualidad, dichas fuerzas, sobre todo las colombianas, han alcanzado un sitio de prestigio en la región gracias a sus acciones decisivas (Lauriani, 2017, p. 26).

El empleo de las Fuerzas Especiales en escenarios de guerra asimétrica y guerra híbrida

A partir del análisis doctrinal realizado hasta este punto, es posible afirmar que las FF. EE. se caracterizan entonces por enfocarse en operaciones de alcance

estratégico, con una seguridad mayor que cualquiera operación convencional, sencilla, sorpresiva y veloz, a partir del desarrollo a fondo de la flexibilidad y la adaptabilidad, con una altísima autonomía, iniciativa de combate y clara innovación. Estas características permiten que estas unidades logren un mayor impacto y más decisivo que unidades convencionales mucho más grandes.

Respecto al enfoque operacional, las FF. EE. desarrollan capacidades críticas para desenvolverse en escenarios de guerra especial y realizar ataques con precisión quirúrgica. Las primeras se caracterizan por que se desarrollan en ambientes operacionales permisivos, inciertos u hostiles, por sí mismas o en conjunción con otras formaciones, mientras que las segundas son acciones precisas, limitadas y veloces, con el objetivo de capturar, abatir, controlar o recuperar algún objetivo de interés operacional o estratégico.

Adicionalmente, las agrupaciones de FF. EE. se conciben para operar en ambientes operacionales y en misiones que implican una clara limitación de tiempo, un obligatorio aislamiento de otros componentes, la permanente necesidad de explotar oportunidades a conveniencia, una obligada descentralización en la ejecución de la misión, una permanente iniciativa y una fuerte interdependencia entre equipos especiales para sincronizar o complementar esfuerzos. Solamente así, las agrupaciones de FF. EE. se proyectan hacia el éxito operacional.

Justamente, esta concepción se ha aplicado por décadas en ejércitos como el estadounidense o el británico, los cuales desarrollan operaciones de contingencia de pequeña escala que conjugan todas las capacidades de FF. EE., de manera que permiten ver con claridad su alto valor para la guerra asimétrica e híbrida.

Es por ello que una evaluación operacional de las agrupaciones de FF. EE. en distintos contextos puede demostrar que la mayoría ha obtenido resultados notables. Esto se debe a que antes de ejecutar una misión, el planeamiento y, especialmente, el análisis de los cursos de acción conciben escenarios con un gran porcentaje de éxito. Con este propósito, se emplean matrices de información muy detalladas con todas las probabilidades que se pueden presentar en el desarrollo de la misión para evaluar las posibilidades de éxito.

El factor comunicacional, propio de las guerras asimétricas, también se tiene en cuenta en el efecto de las FF. EE. La información sobre las Operaciones Especiales que se entrega a la opinión pública, y que posteriormente llega al enemigo, se comparte de manera restringida para garantizar la eficiencia y la eficacia de la misión, pero también para que el efecto psicológico de la operación pueda ser administrado en función del objetivo político. Por eso, en la mayoría de los casos

no se sabe nada sobre las Operaciones Especiales hasta que son ejecutadas. Es usual que no se proporcione detalles de estas acciones para evitar que la información se fugue hacia organizaciones adversarias, las cuales realizan inteligencia delictiva con los datos que presentan los medios de comunicación y que analizan para contrarrestar a las FF. EE. o para cambiar su *modus delictivo*.

En el contexto contemporáneo, tanto de las guerras asimétricas como híbridas, se encuentran Operaciones Especiales paradigmáticas que demuestran las capacidades y el entrenamiento constante de estas unidades de élite. De allí que sea necesario mantener su evolución y manejar sus intervenciones de forma adecuada, ya que un grupo selecto hace la diferencia en una guerra y en la cantidad de pérdidas de vidas humanas, que muchas veces son innecesarias.

En los diferentes contextos de las guerras, las agrupaciones de FF. EE. han tenido un papel muy importante para defender el Estado o una misión en particular que desarrolla una fuerza multilateral desplegada en cualquier parte del mundo. Si bien es cierto que no todos los Estados cuentan con Fuerzas Militares, estos sí requieren que un país aliado los proteja con sus capacidades especiales, de tal manera que garanticen que no haya acciones hostiles o ataques terroristas de otros Estados u organizaciones.

Al respecto, cabe enfatizar que el enfoque doctrinal de las FF. EE. facilita la interoperabilidad entre los Estados que tengan acuerdos militares o de cooperación, lo cual garantiza que en el futuro puedan reaccionar ante una amenaza de forma coordinada y planeada. Estas peculiares características de interoperabilidad y flexibilidad son muy propias de los adversarios asimétricos cuando construyen sus redes regionales o incluso transnacionales. Así las cosas, las FF. EE. pueden balancear esta condición del adversario mediante el desarrollo de ejercicios militares, los cuales determinan la cooperación y miden las posibilidades que pueden tener las operaciones de FF. EE. en cualquiera de los contextos de guerra u acción contemporánea.

Todo esto no solo fortalece la lucha conjunta contra las amenazas transnacionales que enfrentan los Estados en todo momento, sino que además permite intercambiar información y verificar áreas en temas de interés mutuo, como el terrorismo, el narcotráfico, el tráfico humano y el tráfico de armas. Por consiguiente, se debe continuar y mejorar en este proceso de transformación y adaptación de las FF. EE. a los nuevos escenarios que atentan contra la seguridad nacional e integral en el contexto contemporáneo del siglo XXI, altamente marcado por la asimetría y la hibridez.

De tal manera, las operaciones de las FF. EE. en la mayoría de los países consisten en misiones de guerra híbrida y asimétrica –no convencional–, como defensa interna extranjera, reconocimiento especial, acción directa, lucha contra el terrorismo, búsqueda y rescate de combate, lucha contra el narcotráfico, rescate de rehenes, asistencia humanitaria, operaciones de información y operaciones psicológicas. Las operaciones de FF. EE. tienen la capacidad de garantizar que van a ser los primeros en el terreno o incluso que ya se van a encontrar en un lugar de crisis cuando una amenaza hasta ahora comienza a organizarse.

Conclusiones

La guerra contemporánea se caracteriza básicamente por dos tipos de confrontaciones, la asimétrica y la híbrida. Estas guerras tienen un componente muy irregular, flexible y deslocalizado, basado en agrupaciones ágiles, fácilmente mimetizables y con alto poder de afectación. Sin duda alguna, este tipo de adversario representa una seria dificultad para las unidades convencionales, pues su vasto poder y gran tamaño poco ofrecen como ventaja.

En respuesta a esta dificultad, las agrupaciones de FF. EE. son justamente las unidades que más se aproximan a los conceptos operacionales que es necesario aplicar en la asimetría y la hibridez. Su flexibilidad, reducido tamaño y gran poder de fuego, combinado con las capacidades de sostenibilidad operacional, les permiten comprender y combatir con éxito a organizaciones adversarias en estos ambientes operacionales.

En ese sentido, las agrupaciones de FF. EE. no solo son uno de los activos más importantes de las Fuerzas Militares colombianas, sino que por su experiencia, doctrina, formación y logros en combate ofrecen una ventana de oportunidades para el Estado. Es clara entonces la posibilidad de que este activo aporte a la seguridad y la defensa del país y se convierta en referente internacional de profesionalismo, capacidades y poder militar.

Referencias

- Aznar, F. (2015, 25 de noviembre). *Las generaciones de guerras: Guerras de primera generación (I)* [Documento de Análisis, n.º 54]. Instituto Español de Estudios Estratégicos. <https://tinyurl.com/5yca9se5>
- Chomsky, N. (2000). *Rogue States: The rule of force in world affairs*. Pluto Press.
- Colom, G. (2012). Vigencia y limitaciones de la guerra híbrida. *Revista Científica General José María Córdova*, 10(10), 77-90. <https://doi.org/10.21830/19006586.228>
- García Guindo, M., Martínez, G., & González, V. (2015). *La guerra híbrida: Nociones preliminares y su repercusión en el planeamiento de los países de las organizaciones occidentales* [Documento de Trabajo]. Instituto Español de Estudios Estratégicos. <https://tinyurl.com/bdh8njt9>
- Herman, P. (1997). Asymmetric warfare: Seizing the threat. *Low Intensity Conflict & Law Enforcement*, 6(1), 23-45.
- Hoffman, F. (2009). Hybrid warfare and challenges. *Joint Force Quarterly*, 52(1), 34-39. <https://tinyurl.com/42ne9y2d>
- Kaldor, M. (2001). *Viejas y nuevas guerras*. Tusquets.
- Lauriani, C. (2017). Operaciones Especiales: Una respuesta multidimensional al problema de seguridad multidimensional de Latinoamérica. *Military Review*, (segundo trimestre), 20-30. <https://tinyurl.com/5n8umnz>
- Lind, W. (2005). Comprendiendo la guerra de cuarta generación. *Military Review*, (enero-febrero), 11-17. <https://tinyurl.com/y2uzpd6d>
- Metz, S., & Johnson, D. (2001). *Asymmetry and US Military Strategy: Definition, background and strategic concepts*. Strategic Studies Institute. <https://apps.dtic.mil/sti/tr/pdf/ADA387381.pdf>
- Miron, M. (2019). La guerra irregular, insurgencia y cómo contrarrestarla: Una perspectiva comparativa entre los enfoques centrados en el enemigo y en la población. *Revista Científica General José María Córdova*, 17(27), 457-480. <https://doi.org/10.21830/19006586.497>
- Münkler, H. (2002). *Viejas y nuevas guerras: Asimetría y privatización de la guerra*. Siglo XXI.
- Sánchez, J., Montero, L., Ardila, C., & Ussa, A. (2012). Discusión epistemológica de la guerra asimétrica: Adopción contemporánea de la asimetría interestatal. *Revista Científica General José María Córdova*, 10(10), 91-05. <https://doi.org/10.21830/19006586.229>
- Sigüeñas, O. (2018). Tareas operacionales de las Fuerzas Especiales: Optimizar el desempeño operativo del componente de Fuerzas Especiales del Comando Especial del valle de los ríos Apurímac, Ene y Mantaro. *Air & Space Power Journal*, (cuarto trimestre), 55-61. <https://tinyurl.com/u75yxtnw>
- Trejo, P. (2018). Tropas de Operaciones Especiales: Herramienta útil para las guerras del futuro. *Visión Conjunta*, 10(19), 47-55. <https://tinyurl.com/ycxd2vuh>

- Tung, M. T. (1967). *Selección de escritos militares*. Ediciones en Lenguas Extranjeras.
- Verstrynge, J. (2005). *La guerra periférica y el Islam revolucionario: Orígenes, reglas y ética de la guerra asimétrica*. El Viejo Topo.
- Walker, R. (1998). *SPEC FI: The United States Marine Corps and Special Operations*. Naval Postgraduate School.

Capítulo 2

En la mente del estratega: identificando la estrategia aplicada al sistema de adquisición de blancos*

DOI: <https://doi.org/10.25062/9786287602809.02>

Helver Orlando Cepeda Daza
Oscar Leonardo Reyes Pulido

Escuela Superior de Guerra "General Rafael Reyes Prieto"

Resumen: El alcance estratégico de los efectos que tienen las unidades de Fuerzas Especiales colombianas ha permitido destacarlas como una herramienta relevante que puede ser empleada en el rango de operaciones militares. El alcance de los objetivos de naturaleza estratégica son el resultado de la combinación de experiencia y aplicación de la doctrina. Este pensamiento creativo, desarrollado por estrategias de las Fuerzas Especiales, ha hecho posible que evolucionen en materia táctica y en el arte operacional. Este estudio describe el enfoque sistémico de la estrategia aplicada a una de las capacidades críticas de las operaciones de Fuerzas Especiales, como son los ataques con precisión quirúrgica. A través del método científico militar DOMPILEM, se analiza la capacidad construida por las Fuerzas Especiales colombianas. Finalmente, se presenta un modelo conceptual que identifica las capacidades estratégicas del proceso extraídas de estudios de caso con características interoperables para otras unidades de Fuerzas Especiales.

Palabras clave: adquisición de blancos; arte operacional; estrategia; interoperabilidad; operaciones especiales.

* Este capítulo es resultado de investigación adscrito al proyecto "Naturaleza de la guerra contemporánea. Retos y oportunidades de las Fuerzas Especiales y la Inteligencia", adscrito al Departamento Ejército de la Escuela Superior de Guerra, inscrito en la línea de investigación "Naturaleza de la guerra, terrorismo, nuevas amenazas", que forma parte del grupo de investigación Centro de Gravedad, categorizado en A por Minciencias, con código COL0104976. Los puntos de vista pertenecen a los autores y no reflejan necesariamente los de las instituciones participantes.

Helver Orlando Cepeda Daza

Teniente Coronel de Fuerzas Especiales de Colombia con doce años de experiencia como Operador Especial. Magíster en Estrategia y Geopolítica, Escuela Superior de Guerra "General Rafael Reyes Prieto", Colombia. Especialista en Asuntos de Cooperación en Seguridad y Planeamiento de Operaciones Especiales, Universidad Conjunta de Operaciones Especiales de Estados Unidos - JSOU. Graduado del Centro de Guerra Especial y Escuela de Fuerzas Especiales John F. Kennedy en Fort Liberty, Estados Unidos. Profesional en Ciencias Militares, Escuela Militar de Cadetes "General José María Córdova", Colombia. Oficial de enlace multinacional ante el Comando de Operaciones Especiales de los Estados Unidos - SOCOM. Contacto: helver.cepeda@buzonejercito.mil.co

Oscar Leonardo Reyes Pulido

Mayor (R) del Ejército Nacional de Colombia. Magíster en Seguridad y Defensa Nacionales, Escuela Superior de Guerra "General Rafael Reyes Prieto", Colombia. Especialista en Derechos Humanos y Derecho Internacional Humanitario, Universidad Externado de Colombia. Profesional en Ciencias Militares, Escuela Militar de Cadetes "General José María Córdova", Colombia. Abogado, Universidad Militar Nueva Granada, Colombia. Docente investigador, Escuela Superior de Guerra "General Rafael Reyes Prieto", Colombia. <https://orcid.org/0000-0001-6341-0283> - Contacto: oscar.reyesp@esdeg.edu.co

Citación APA: Cepeda Daza, H. O., & Reyes Pulido, O. L. (2024). En la mente del estratega: Identificando la estrategia aplicada al sistema de adquisición de blancos. En L. A. Montero Moncada & O. A. Garzón Gómez (Eds.), *Comandos: Retos de las Fuerzas Especiales e Inteligencia en la guerra contemporánea* (pp. 33-64). Sello Editorial ESDEG. <https://doi.org/10.25062/9786287602809.02>

COMANDOS: RETOS DE LAS FUERZAS ESPECIALES E INTELIGENCIA EN LA GUERRA CONTEMPORÁNEA

ISBN impreso: 978-628-7602-79-3

ISBN digital: 978-628-7602-80-9

DOI: <https://doi.org/10.25062/9786287602809>

Colección Seguridad y Defensa

Sello Editorial ESDEG

Escuela Superior de Guerra "General Rafael Reyes Prieto"

Bogotá D.C., Colombia

2024



Introducción

La arquitectura organizacional de las Fuerzas de Operaciones Especiales (en adelante FF. EE.) colombianas se ha caracterizado por que evoluciona de forma constante para realizar operaciones de naturaleza no convencional. Estas modificaciones les han permitido adaptarse a factores predominantes en el ambiente operacional contemporáneo, como la evolución de la amenaza, y los ambientes geográficos más adversos, hostiles y dinámicos. Asimismo, la constante evaluación de los sistemas de amenaza les ha permitido descifrar acciones tácticas exclusivas en tiempo, espacio y propósito para cumplir objetivos de repercusiones estratégicas en ambientes no permisivos, inciertos y negados.

Específicamente, este trabajo aborda la evolución de las capacidades tácticas de las FF. EE. desde una metodología científica que la doctrina militar describe como DOMPILEM: Doctrina, Organización, Material, Personal, Instalaciones, Liderazgo y Educación, Entrenamiento y Mantenimiento¹. Además, se tiene en cuenta que si bien la aplicación del nivel estratégico –en el cual se gestiona la interdependencia y la integración– en el arte operacional ha sido consuetudinario, esto no desdibuja su importancia en los procesos de enseñanza, que es empleado por modelos como el del Reino Unido (Montero et al., 2019).

En este sentido, dado que este modelo británico también ha influido los procedimientos, tácticas y técnicas de las FF. EE., el interrogante que motivó este estudio es el siguiente: ¿Cómo las características derivadas del proceso de adquisición de blancos de la organización de FF. EE. colombianas para lograr los objetivos estratégicos garantizan un grado de interoperabilidad con otras FF. EE.?

¹ En la Organización del Tratado del Atlántico Norte (OTAN) pueden incluir una "I" para referirse a "Interoperabilidad".

A fin de examinar el interrogante, este capítulo aborda la evolución de la estrategia empleada por las FF. EE. dentro del marco conceptual estratégico. Además, analiza cómo este último se adaptó a las necesidades del conflicto y de las políticas de seguridad y defensa, pues ineludiblemente estas políticas públicas trazan los designios del “cómo” y del “estado final deseado”. Posteriormente, se estudia la capacidad que tienen las FF. EE. con el propósito de contribuir a una descripción del caso colombiano con una visión holística. Para esto se emplea el DOMPILEM, puesto que la organización de FF. EE. buscó refinar todos los componentes de esta metodología para que el proceso de selección de blancos fuese exitoso.

Finalmente, con base en una aproximación descriptiva de estudios de caso, se analizan las características del proceso de adquisición de blancos que emplean las FF. EE. para que sean efectivas e interoperables dentro de las Fuerzas Militares. Además, se estudia de qué manera este modelo contribuye a alcanzar los logros estratégicos del Comando Superior.

El horizonte descriptivo propuesto en este capítulo pretende iluminar las aproximaciones únicas que tiene la estrategia de las FF. EE. para desarrollar una operación militar. El análisis de los casos concretos se efectuó siguiendo la orientación del método diseñado por Yin (1989; citado por Martínez, 2006), quien señala que los estudios de caso pueden ser descriptivos “si lo que se pretende es identificar y describir los distintos factores que ejercen influencia en el fenómeno estudiado” (Martínez, 2006, p. 171).

Además, este documento académico pretende aportar referencias para el *Manual de Campaña de Fuerzas Especiales MCE 6-05 Integración, Interoperabilidad e Interdependencia de las Fuerzas Especiales*, el cual se constituirá en un documento doctrinal que proyecte la eficiencia de combate de las FF. EE. en su interacción dinámica con las unidades de Fuerzas convencionales y las FF. EE. de otros componentes de las Fuerzas Militares para ejecutar operaciones de naturaleza conjunta y combinada.

De acuerdo con el *Manual Fundamental del Ejército MFE 3-05 Operaciones de Fuerzas Especiales* (Ejército Nacional de Colombia, 2017a), en la clasificación de las operaciones se pueden presentar *Operaciones Conjuntas*, cuando se realizan con otras Fuerzas, por ejemplo FF. EE. del Ejército y FF. EE. de la Armada Nacional, y *Operaciones Combinadas*, cuando se ejecutan con países aliados extranjeros. Este último es el caso del ejercicio Panamax, una operación militar realizada por el Comando del Ejército Sur de los Estados Unidos que pretende desarrollar una capacidad disuasiva ante cualquier amenaza al Canal de Panamá.

Descripción retrospectiva contemporánea de la organización de las Fuerzas Especiales colombianas

La literatura especializada colombiana ha identificado singulares factores de éxito que son esenciales para garantizar la relevancia de las Operaciones Especiales en el marco de la estrategia militar nacional y general. Entre los trabajos académicos disponibles resulta de suma importancia mencionar el estudio que la Escuela Superior de Guerra “General Rafael Reyes Prieto” (ESDEG) publicó con el título de *El poder terrestre: ejércitos y guerras del siglo XXI*, el cual señala algunas condiciones del ambiente político-militar en el nivel estratégico que deben ser consideradas entre los factores de éxito, tales como “la identificación de capacidades críticas enemigas para formular estrategias militares efectivas, [...] y la transformación de las FF. MM. y sus capacidades a través de la innovación” (Montero et al., 2019, p. 122).

Al respecto, es oportuno mencionar en este momento las dos capacidades críticas que las FF. EE. han desarrollado en el contexto del conflicto colombiano: los ataques de precisión quirúrgica y la guerra especial. Estas capacidades críticas sirven como punto de partida para visualizar cuál fue el enfoque que tuvieron las FF. EE. para realizar el proceso de innovación en la selección de blancos y por qué puede llegar a ser exitoso.

La organización de las FF. EE. ha mantenido un crecimiento sustancial y sostenido desde 1970, cuando el Batallón de Infantería N.º 29 “Rifles” se transformó en la “Agrupación de Fuerzas Especiales Hermanos Almeyda”, la primera unidad con capacidades diferenciales (Muñoz & Cano, 2020). Este proceso permitió una innovación trascendental en las capacidades militares de las FF. EE. que evolucionó la manera como se empleaba del poder terrestre. Esta transformación integral le ha permitido a la organización de FF. EE. mantenerse a la vanguardia para atender las exigencias que implica salvaguardar la seguridad y la defensa de la soberanía nacional. Además de estos cambios, las FF. EE. han podido trascender gracias a su alineación con las diferentes políticas de seguridad del Ejecutivo, lo que les permite convertirse en una opción polivalente para atacar centros de gravedad en todo el rango de operaciones militares.

En agosto del año 2002, entre los apartes de la Política de Seguridad y Defensa Democrática (2002-2010) se destaca la importancia y la proyección de una Inteligencia robusta y con capacidades de coordinación e integración para garantizar su eficiencia. Específicamente, la doctrina denomina este aspecto como *interdependencia*, la cual es definida por el *Manual Fundamental de Referencia del*

Ejército MFRE 3-05 Operaciones como la relación de dependencia entre elementos con el fin de maximizar sus efectos complementarios y de refuerzo (Ejército Nacional de Colombia, 2017c).

Ahora bien, la política de seguridad permite alinear los intereses de la estrategia de seguridad nacional con los objetivos estratégicos del Gobierno. Así, en el año 2002 el Ejecutivo estableció que se debían mejorar los sistemas de recolección, análisis y difusión de Inteligencia, con el fin de garantizar la sinergia operacional que les permite a las Fuerzas Militares recolectar información para poder operar de manera oportuna con el fin de garantizar el alcance de objetivos con repercusiones estratégicas.

Alineado con esa visión estratégica, en el año 2002 el Comandante General de las Fuerzas Militares emitió la orden de crear un grupo interinstitucional denominado “Cancerbero”, un elemento de Inteligencia accionable en el cual participaba el Ejército Nacional, la Armada Nacional, la Fuerza Aérea Colombiana, la Policía Nacional y el Departamento Administrativo de Seguridad (DAS), cuyo objetivo permanente era neutralizar Objetivos Militares de Alto Valor Estratégico (OMAVE) empleando las capacidades críticas de las FF. EE.

Sin lugar a duda y en el contexto de la estrategia, se estableció un propósito que el estrategia concibió dentro de su diseño y arte operacional como el Estado Final Militar Deseado. Ineludiblemente, encontró que era necesario optimizar los medios ya existentes y presentar una innovadora y determinante capacidad, como era el reconocimiento de largo alcance, de manera que el diseño y la implementación permitieran ejecutar las operaciones de FF. EE. con inteligencia recolectada por ellas mismas.

Como unidades orgánicas del Comando de Operaciones Especiales del Ejército (COESE), el Comando del Ejército vio la necesidad de crear una unidad que tuviera pequeños grupos con capacidad de realizar operaciones de reconocimiento especial y acción directa. Así se conformaron unidades con personal del Batallón de Fuerzas Especiales N.º 1 y se invitó a las demás unidades del Ejército Nacional a participar en el proceso de selección. Este último contó con la asesoría del grupo militar de los Estados Unidos, quienes proporcionaron equipo de alta tecnología y materiales distintivos que permitiesen operar en ambientes militarmente negados, tales como equipos de comunicación con tecnología de capacidad satelital.

De esta manera se creó el Batallón de Comandos N.º 1 “Ambrosio Almeida”, una unidad con capacidades casi mitológicas, fantasmas de la selva, personas con una perseverancia y un dominio de sí mismas difíciles de imaginar para la época, además sus habilidades en reconocimiento de OMAVE solo era comparado

con su innovadora organización. De esta manera, pequeños equipos autosuficientes comenzaron a marcar un hito en el desarrollo de misiones especiales.

Ahora bien, dado que una unidad tan pequeña necesita fuerzas de reacción inmediata con capacidades aerotransportadas y de asalto aéreo inherentes a su organización, en el año 2003 se creó una unidad con las características más propias del soldado colombiano, es decir, su tenacidad e ímpetu de combate. De esta manera, un poder de combate abrumador, agilidad y versatilidad fueron las capacidades distintivas e inherentes a la creación y activación de la Agrupación de Lanceros Aerotransportada (AGLAN).

Para cumplir los objetivos de alto valor estratégico, es decir, el estado final deseado, se generó entonces un set de condiciones innovadoras compuesto por un bisturí (el Batallón de Comandos, BACOA) y un martillo (la AGLAN), unidades que se destacaron en ese entonces ejecutando ataques de precisión quirúrgica. En ese momento los elementos esenciales de inteligencia que requerían los comandantes en todos los niveles eran suplidos por equipos que suministraban información sobre áreas donde otras unidades e inclusive otras capacidades institucionales no podían llegar.

Durante ese mismo año se vio la necesidad de adherir unidades con habilidades específicas para mejorar el COESE, de manera que el 17 de mayo del 2005 pasaron a integrar este comando la Agrupación de Fuerzas Especiales Antiterroristas Urbanas (AFEAU) y el Batallón de Fuerzas Especiales de Infantería de Marina (BFEIM). Como resultado de esta organización se estableció primero el Comando Unificado de Operaciones Especiales (CUNOE) y posteriormente el Comando Conjunto de Operaciones Especiales (CCOPE).

Con la creación de estas unidades y con el mando operacional del Comando General de las Fuerzas Militares (CGFM), se afectó el direccionamiento estratégico de las organizaciones narcoterroristas gracias a la neutralización de mandos medios, pero no se cumplió con la misión de atacar el centro de gravedad, es decir, los OMAVE (CCOES, 2014).

Como consecuencia se iniciaron procesos de transformación e innovación en las FF. EE. y, tras una visita del Ministro de Defensa Nacional colombiano al ejército de Israel, se implementó el Grupo Nacional de Planeación de Operaciones Especiales e Inteligencia, que se basó en el modelo de este país visualizado para el año 2007. En este contexto, por órdenes del CGFM se creó la Jefatura de Operaciones Especiales Conjuntas, integrada por 22 oficiales, 24 suboficiales y 2 civiles, todos integrantes del Ejército, la Armada, la Fuerza Aérea, la Policía y el DAS (CCOES, 2014).

Así, durante los años 2007 y 2008 se logró afectar el centro de gravedad de la organización narcoterrorista denominada Fuerzas Armadas Revolucionarias de Colombia (FARC), mediante el planeamiento y el desarrollo de operaciones especiales. Entre estas se destaca la operación “Sol Naciente”, que constituye una muestra de la integración de unidades de las FF. EE. y de la efectividad de la Fuerza Aérea (Brigada de Fuerzas Especiales, 2015).

Con el fin de mejorar las capacidades de las unidades de FF. EE., también se solicitó asesoría externa para crear un comando de operaciones especiales. Así, en los meses de septiembre y diciembre de 2008 se realizaron reuniones con diferentes personalidades y asesores de otras naciones para generar compromisos de entendimiento, desarrollar la guía inicial, proyectar la misión, la visión y la aprobación de la organización recomendada. Este trabajo se extendió hasta los meses de enero y febrero de 2009, en los cuales se consolidó la estructura organizacional, los roles y las funciones específicas del CCOES. Finalmente, el 27 de mayo de 2009, el CGFM desactivó el Comando Conjunto de Operaciones Especiales (CCOPE) y creó el Comando Conjunto de Operaciones Especiales (CCOES).

En esta evolución también es importante citar el Comité de Revisión Estratégica que se realizó en el año 2014, donde se trazaron metas importantes –como actualizar la doctrina y adoptar el planeamiento basado en capacidades– para definir el futuro de las FF. EE. y mantenerlas a la vanguardia. Posteriormente, en el 2016 se estableció la doctrina militar vigente, la cual define las Operaciones de Fuerzas Especiales como una de las competencias distintivas del Ejército Nacional (Ejército Nacional de Colombia, 2016b).

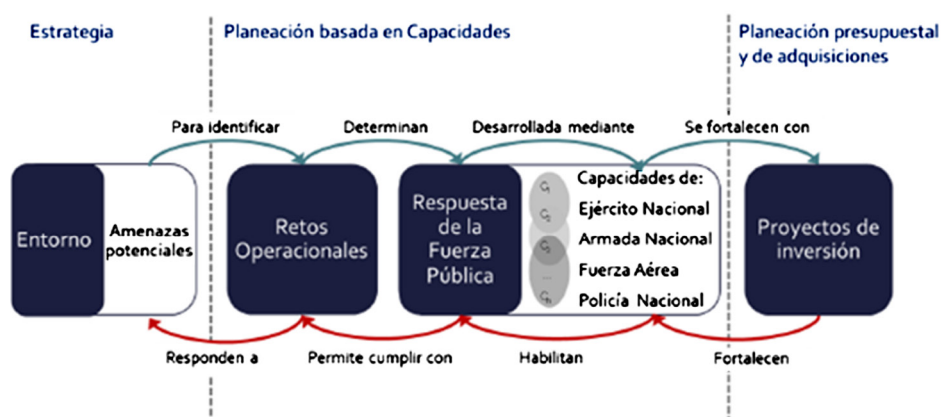
Durante los años 2015 y 2016, el CGFM inició el proceso para consolidar la estructura organizacional de las FF. EE. Mediante la publicación de resoluciones y disposiciones de fuerza, el CGFM suprimió y reorientó en su dependencia al mando algunas de las unidades más emblemáticas de las FF. EE., los hombres considerados con la mejor preparación para la guerra y para afrontar las amenazas en contra del Estado colombiano.

Finalmente, en diciembre de 2016, el Comandante del Ejército Nacional creó la División de Fuerzas Especiales del Ejército Nacional (DIVFE). Como se observa, en el contexto del pensamiento estratégico es evidente la naturaleza pragmática de la cultura estratégica que han empleado las FF. EE. colombianas, pues sus decisiones acertadas y evolución le han permitido adaptarse e innovar en escenarios que se caracterizan por una alta volatilidad, incertidumbre, complejidad y ambigüedad. Así lo describen Gallardo y Faundes (2014): “Además de comprender el contexto, el pensamiento estratégico busca los lineamientos para influenciar y dar forma al escenario” (p. 10).

Análisis de capacidad DOMPILEM de las FF.EE. colombianas y su interdependencia con el proceso de adquisición de blancos

En primer lugar, es valioso resaltar que el proceso de selección y priorización de blancos es el resultado de la construcción de una capacidad, de allí que sea importante describir la capacidad que ha desarrollado el Ejército Nacional con base en unos pilares y teniendo en cuenta sus capacidades y limitaciones (figura 1). En cumplimiento de las directrices establecidas por el Ministerio de Defensa Nacional (MDN) en este modelo de planeamiento, la organización de las FF. EE. optimizó los recursos asignados y creció alrededor de una visión prospectiva de la amenaza, de manera que no solo se adaptaban, sino que además se convirtieron en una competencia que el Ejército Nacional declaró como distintiva en el año 2016 (Ejército Nacional de Colombia, 2017a).

Figura 1. Metodología de planeación basada en capacidades.



Fuente: MDN (2016).

El análisis de la capacidad que emplean las FF. EE. para seleccionar y priorizar los blancos se realizará desde la perspectiva integral DOMPILEM, la cual consiste en una metodología científica que utiliza el Ejército Nacional para evaluar, innovar y modernizar las capacidades. Esta herramienta abarca además la doctrina, la organización, el material, el personal y la infraestructura con las que cuenta la unidad para desarrollar sus capacidades críticas, como son la guerra especial y los ataques de precisión.

Doctrina

La nueva doctrina del Ejército Nacional define las Operaciones Especiales (OO. EE.) como acciones militares conducidas por unidades organizadas, entrenadas, equipadas y certificadas, las cuales pueden ejecutar acciones en tipos de ambientes hostiles, militarmente negados y políticamente sensibles (Ejército Nacional de Colombia, 2017c).

Entre las OO. EE. se distingue una serie de operaciones que, a su vez, forman parte de las dos capacidades críticas de las FF. EE.: la guerra especial y los ataques de precisión quirúrgica. Estas dos capacidades críticas se desarrollan dentro de un marco de referencia común e interoperable de acuerdo con parámetros y lineamientos claros, lo cual les permiten integrar y emplear conceptos de organización, planeamiento y ejecución para realizar con éxito las OO. EE.

Los hombres de las FF. EE. del Ejército Nacional se rigen por rigurosos documentos estandarizados militarmente que definen las tácticas, las técnicas y los procedimientos que deben emplear las unidades de naturaleza diferente, “especial”. Estos documentos trascienden a pilares que sostienen la legitimidad de la organización y que constituyen la doctrina, a la cual el *Manual Fundamental del Ejército MFE 1-01* define como los “principios fundamentales con sus correspondientes tácticas, técnicas, procedimientos y términos empleados para la guía y conducción de operaciones militares” (Ejército Nacional de Colombia, 2016a, p. 1). Para la organización de las FF. EE., estos principios son traducidos como documentos estandarizados en el nivel local y regional con el propósito de que las Fuerzas Militares aliadas tengan un lenguaje común interoperable en el marco común del desarrollo de operaciones combinadas.

La experiencia obtenida del conflicto colombiano ha permitido desarrollar esta doctrina actual, como señala el señor Coronel de la Reserva Activa Pedro Rojas Guevara (2017), director del Centro de Doctrina del Ejército Nacional entre 2015 y 2018, magíster en Seguridad y Defensa Nacional, analista y catedrático en temas de seguridad y defensa. En su artículo “Doctrina Damasco: eje articulador de la segunda gran reforma del Ejército Nacional de Colombia”, afirma:

La doctrina actual del Ejército de Colombia es el producto de un cúmulo de influencias derivadas de cincuenta años de conflicto armado. De aparente influencia americana en la parte formal, ha tenido un desarrollo más ligado con lo fáctico, dentro de un contexto asimétrico, que con lo teórico. (Rojas, 2017, p. 114)

Se evidencia entonces que estos documentos no solo han permitido conceptualizar la intrepidez y las innovadoras acciones que han ejecutado las unidades de FF. EE., sino que además comprenden categorías de información que describen la ejecución de los procesos, es decir, el *know how* de las capacidades críticas de las FF. EE. Específicamente, Llobregat (2007) y Vilorio et al. (2008), citados por Castaño y Arias (2015), explican que el *know how* es el “saber hacer organizacional que comprende aquellos conocimientos, procesos, procedimientos y técnicas que derivan en la consecución de un servicio que es diferente y difícil de copiar por las demás organizaciones” (p. 154). En este sentido, los principales documentos que sintetizan este saber son:

- Manuales Fundamentales del Ejército (MFE), en los cuales se describe la filosofía de las FF. EE., sus principios, fundamentos e imperativos, así como aquellos elementos característicos de los ambientes operacionales donde se pueden emplear.
- Manuales de Referencia del Ejército (MFRE), los cuales consisten en documentos doctrinales de más detalle que describen los tipos de operaciones que pueden ser ejecutadas por las FF. EE. y sus métodos de planeamiento. Además, se refieren al nivel operacional-táctico y evidencian tanto las capacidades como las cualidades de la organización de FF. EE.
- Manuales de Campaña (MCE): describen las capacidades específicas que tienen las operaciones de las FF. EE. y amplían la información contenida en los MFRE sobre capacidades específicas. Los MCE se extienden en los conceptos que la organización necesita profundizar.
- Manuales de Técnicas del Ejército (MTE): describen en detalle las formas o métodos no obligatorios que emplean las unidades militares para llevar a cabo las misiones impuestas por comandos superiores. Estas técnicas se aplican de acuerdo con el juicio disciplinado sobre las condiciones operacionales que el escenario impone.
- Manuales de Entrenamiento Militar (MEM): describen características técnicas muy precisas que detallan las tareas específicas que se deben ejecutar. Un ejemplo de este tipo de documentos es un manual que describe las técnicas y los procedimientos que se utilizan en una operación de salto militar en caída libre, un procedimiento que exige conocimientos muy precisos.

Organización

En los números de las FF. EE. se pueden contar alrededor de 4000 operadores especiales con capacidades críticas en ataques de precisión quirúrgica y guerra especial, pero no se pueden destacar lugares específicos que caractericen su participación debido a circunstancias relacionadas con su arquitectura organizacional. Al ser parte del componente terrestre del CCOES, no tienen un teatro de operaciones asignado porque se trata de un Comando Conjunto Funcional, propiedad que le permite realizar operaciones en todo el territorio nacional, sujetos a tiempos de ejecución eficientes que garanticen la respuesta militar que el objetivo estratégico requiere.

Específicamente, la DIVFE nació en el 2016 y junto a otros componentes de la Fuerza Aérea y la Armada Nacional representan un tridente estratégico para las Fuerzas Militares de Colombia que, a través del CCOES, refleja la interoperabilidad, la interdependencia y la naturaleza conjunta de la organización. Estas propiedades características son parte del ADN de la organización y le permiten explotar capacidades únicas y exclusivas, además de recursos estratégicos en modo, tiempo y lugar decisivos en todo el rango de las operaciones militares.

Además, la DIVFE, como componente terrestre del CCOES, está soportada en una estructura moderna y funcional para cumplir con todos los requerimientos que imponen las OO. EE. que deben realizar las FF. EE., por cuanto es la unidad encargada de centralizar su planeamiento. En su búsqueda constante de perfeccionar el proceso para la adquisición de blancos, la DIVFE emplea un sistema que se describe con la sigla F3EAD: *focus, fix, finish, exploit, analyze and disseminate*, el cual le permite anticipar y descifrar los escenarios ambiguos en los que delinque la amenaza (Ejército Nacional de Colombia, 2017a).

Este proceso hace posible que la DIVFE identifique, localice y neutralice la amenaza, así como realizar análisis que están sujetos a procedimientos judiciales estrictos y que le permiten hacer estudios prospectivos sobre el *modus operandi* de la amenaza terrorista. Además, con su aplicación puede realizar un proceso de selección y priorización de blancos (PSPB) a través de apreciaciones dinámicas rigurosas, con lo cual está en capacidad de hacer una preparación de inteligencia del campo de combate (PICC) alineada con los requerimientos de información críticos que el comandante requiere para su toma de decisiones.

En este proceso se debe destacar que las FF. EE. desarrollaron una herramienta de análisis única y exclusiva que resulta determinante en el contexto de las Fuerzas Militares colombianas: el Tanque de Planeamiento de Operaciones Especiales

(TPOE), un enlace entre el arte y la ciencia de la guerra. Específicamente, el TPOE es una célula funcional conformada por personal experto en evaluación y prospectiva, quienes conforman equipos altamente entrenados y versátiles con las capacidades necesarias para analizar los distintos ambientes operacionales donde van a ejecutar sus operaciones los batallones de FF. EE. (Ejército Nacional de Colombia, 2017c).

El TPOE somete los cursos de acción que pueden ser viables en la ejecución de una operación a juegos de guerra y a una diversidad de matrices con el propósito de que la ciencia dictamine si las variables de la misión están bien o no consideradas. Por ejemplo, dado que para realizar una operación de asalto aéreo la meteorología tiene un papel fundamental en la inserción y la extracción de las unidades, en este ciclo de planeamiento el TPOE explora patrones y matrices sobre las condiciones atmosféricas y, con un experto meteorólogo de la Fuerza Aérea Colombiana, establece las mejores ventanas u horarios para ejecutar la operación. Como se observa, en este nivel de aplicación del poder militar la conjuntos tiene un papel determinante.

Cabe señalar que la capacidad más robusta del TPOE es definir y preparar el ambiente operacional que afecta una operación. Su habilidad para identificar los requerimientos y los valores críticos en ese ecosistema se refleja en la experticia que tiene para detectar las limitaciones, las necesidades, los requerimientos iniciales, las características y las propiedades del terreno, así como el tiempo atmosférico en un área geográfica. Es decir, el TPOE no solo determina “el qué”, sino también todos los factores que pueden afectar la ejecución de una misión, lo cual sin duda es esencial para desarrollar los cursos de acción dinámicos y apropiados para las OO. EE.

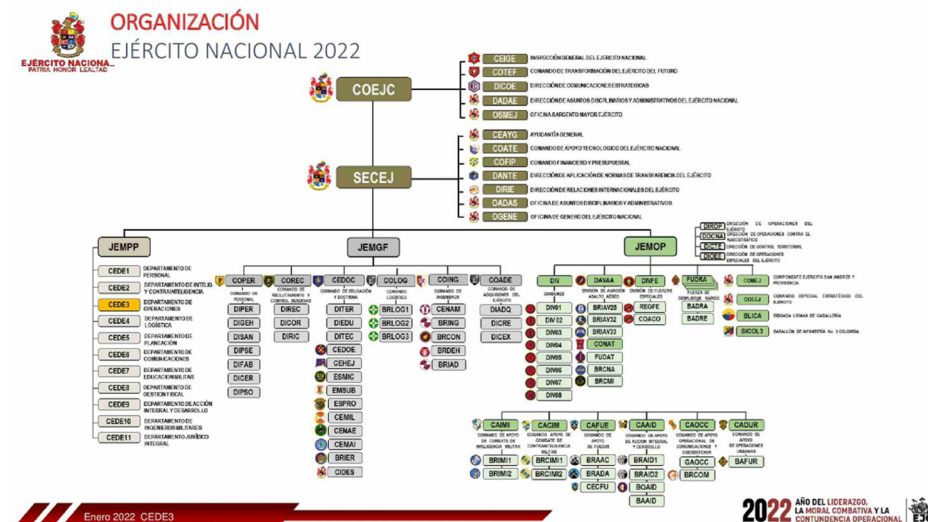
Además, sus capacidades para analizar el terreno y sus efectos en las acciones son parte esencial en la ejecución de las operaciones. Por esta razón, el pensamiento creativo y crítico del TPOE evoluciona constantemente con el fin de refinar su habilidad para ejecutar el proceso militar para la toma de decisiones y, de esta manera, desarrollar una integración temprana con la premisa de construcción del blanco.

En este contexto, los TPOE son responsables de realizar los Procesos de Operaciones de FF. EE., los cuales consisten en una serie de pasos para analizar y determinar los cursos de acción para la toma de decisiones. Esto les permite acertar y minimizar los riesgos en la ejecución de las misiones que se desarrollan en los diversos ambientes operacionales contra Blancos de Alta Retribución (HPT, por la sigla en inglés de *High-Pay off Target*) y sus centros de gravedad a lo largo y ancho de la geografía nacional.

Derivado del trabajo de los TPOE, se puede destacar que la DIVFE cuenta con una amplia experiencia, la cual se refleja en el planeamiento de más de doscientas operaciones de FF. EE., y que su estructura le permite ejecutar operaciones conjuntas con unidades que, bajo el mando del CCOES, son interoperables. Precisamente, esta es una de las mayores fortalezas del componente terrestre, que en la estructura generadora de combate depende del Comando de Despliegue del Ejército. Por su parte, las unidades adscritas al CCOES se pueden emplear en cualquier operación a través de relaciones de mando establecidas por la organización, de manera que si un comandante necesita, por ejemplo, habilidades específicas de infiltración en agua, como K-DUCK o K-DROP, a través de la DIVFE puede solicitar al CCOES equipos de reconocimiento especial del Batallón de Fuerzas Especiales de Infantería de Marina dentro del planeamiento y le serán asignadas.

Como se evidencia en la figura 2, la DIVFE es subordinada de la Jefatura del Estado Mayor de Operaciones como elemento generador de fuerza, pero su elemento generador de combate y como componente terrestre depende del CCOES. En este sentido, la DIVFE es una unidad operativa mayor con una amplia gama de capacidades que desarrolla con base en el continuo empleo de sus batallones. Estas habilidades en planeamiento, preparación, ejecución y evaluación permanente de los diferentes ambientes operacionales están descritas en su misión.

Figura 2. Organigrama Ejército Nacional.



Fuente: Ejército Nacional de Colombia (2023).

Finalmente, la DIVFE también está compuesta por regimientos de FF. EE. con capacidades aerotransportadas, los cuales son su elemento generador de combate y un componente generador de fuerza. Esta organización dinámica y autosuficiente le permite al comandante mantener operacionalmente activas las unidades de FF. EE. sin afectar su ciclo de entrenamiento y sostenimiento.

Material

La adquisición del material empleado por la Organización de Fuerzas Especiales es debidamente proyectada por un departamento de planeación de la DIVFE, que realiza un juicioso proceso con el fin último de garantizar que el equipamiento y el mejoramiento se realicen de manera adecuada y oportuna. Así lo señala el libro estructural del CCOES en el proyecto Odiseo, en el cual las adquisiciones de material son ejecutadas de forma organizada e integral para garantizar la interoperabilidad del material adquirido.

Las capacidades operacionales de las unidades de OO. EE. cuentan con un robusto sistema de comunicaciones de tecnología satelital e interoperable con países aliados del hemisferio occidental. Esta tecnología contribuye a que los productos se alineen para que puedan operar en condiciones de sinergia y eficiencia en el intercambio de información. Este innovador sistema de comunicaciones del CCOES le permite enlazar desde unidades en el nivel táctico hasta el comando y control en el nivel estratégico para fortalecer el mando tipo misión en la ejecución de las OO. EE. En este escenario, la transmisión de datos y voz en tiempo real es un punto decisivo esencial para que ejecute sus capacidades críticas.

Por su parte, el componente terrestre del CCOES (es decir, la DIVFE), cuenta con el material necesario para ejecutar OO. EE. que involucren el empleo de medios aéreos. En este sentido, formar parte del CCOES es un elemento multiplicador del poder de combate de la DIVFE, pues le permite operar con una flota estratégica en apoyo de la Fuerza Aérea Colombiana. Gracias a este alto nivel de interdependencia, no solo puede alcanzar bases de lanzamiento a lo largo y ancho del territorio nacional, sino que además cuenta con sistemas de aeronaves remotamente tripuladas y aviones con capacidades de inteligencia, con lo cual logra ventajas en el espectro electromagnético que garantizan su iniciativa operacional. Y aunque estas unidades tienen armamento de última tecnología, este no constituye el aspecto más importante, como lo manifiesta el *motto* "es más importante el *software*, que el *hardware*".

Personal, liderazgo y entrenamiento

El Ejército Nacional ha consolidado a través de su historia una doctrina material, infraestructura y fuertes valores que contribuyen al desarrollo de líderes militares con las capacidades necesarias para conducir operaciones militares en los diferentes niveles de la guerra, los cuales van desde lo táctico hasta lo estratégico militar. A continuación, se describen de manera esquemática los diferentes tipos de entrenamientos con los que cuenta la institución.

Entrenamiento individual

Preparación formal

Es aquella que se recibe en las diferentes escuelas y centros de entrenamiento del Ejército Nacional:

1. *Escuela Militar de Cadetes "General José María Córdova" (ESMIC)*: el alma mater del Ejército Nacional es la encargada de formar integralmente los futuros oficiales del Ejército como líderes comandantes de pelotón, profesionales en ciencias militares y otras disciplinas, con sólidas competencias fundamentales en principios y valores institucionales, en función del desarrollo y la seguridad nacional. La ESMIC forma oficiales para la conducción táctica de unidades y los capacita en el manejo de pequeñas unidades. Esta formación les permite desarrollar habilidades de planeamiento, preparación, ejecución y evaluación de operaciones en situaciones hostiles y condiciones adversas, lo cual fomenta sus habilidades técnicas y tácticas en el comando y control de unidades tipo pelotón o destacamento.
2. *Escuela Militar de Suboficiales "Sargento Inocencio Chincá" (EMSUB)*: tiene la misión de formar a los futuros suboficiales del Ejército multimisión en la Tecnología en Entrenamiento y Gestión Militar, de manera que cuenten con las habilidades para comandar, instruir y administrar escuadras en el nivel táctico.
3. *Escuela de las Armas y Servicios (EAS)*: el Comando del Ejército, mediante la Disposición N.º 007 del 23 de junio de 1980, creó este centro docente para que respondiera exclusivamente a las exigencias académicas de la institución y estructurara la formación profesional de sus cuadros de mando. De esta manera, esta escuela desarrolla cursos de capacitación y especialización para ascenso y técnicas para oficiales de las armas y servicios, así como de formación técnica para suboficiales. Además, establece

pautas de doctrina táctica y técnica para las armas y los servicios hasta nivel batallón.

La misión de la EAS es capacitar de manera integral a los oficiales, subalternos y suboficiales de las Fuerzas Militares como comandantes de unidad fundamental, compañía y miembros de plana mayor mediante la generación, actualización, difusión e implementación de la doctrina a nivel táctico para desarrollar operaciones y maniobras militares que contribuyan a la seguridad, la defensa y el desarrollo del país.

4. *Escuela Superior de Guerra "General Rafael Reyes Prieto" (ESDEG)*: es una Institución de Educación Superior (IES) militar que capacita a los oficiales superiores de las Fuerzas Militares. Es una IES que desarrolla a nivel conjunto habilidades y competencias para sincronizar, integrar y ejecutar planeamientos para la toma de decisiones a nivel conjunto.

Instrucción especializada

Son los cursos que tienen como objeto especializar a quienes van a ejecutar las operaciones de FF. EE. Estos cursos incluyen: lancero, paracaidismo, FF. EE., jefe de salto, explorador y guía de aeronaves, infiltración a gran altura, curso de tiradores de alta precisión, curso de maestro de asalto aéreo y curso de nadador de seguridad.

Además, en el marco de la interoperabilidad y como parte de los programas de cooperación con el Ejército de los Estados Unidos, el CCOES ha desarrollado habilidades avanzadas para ejecutar operaciones de infiltración táctica avanzada. Gracias a esta alianza ha logrado preparar oficiales en el Centro y Escuela de Guerra Especial John F. Kennedy (USAJFKSWCS, por la sigla en inglés de U.S. Army John F. Kennedy Special Warfare Center and School) en estos cursos:

- a. *Military Free Fall Jumpmaster Course (MFFJM)*: la doctrina interoperable y asociada que emplean las FF. EE. les ha permitido crear fortalezas en el entrenamiento avanzado que requieren este tipo de OO. EE. Este exclusivo curso, en el cual personal orgánico de la DIVFE ha participado con oficiales expertos en salto militar en caída libre, se especializa en capacitar a jefes de salto en inspección a paracaidistas de caída libre; procedimientos de emergencia; equipo suplementario de oxígeno; planeamiento de puntos de inserción y alturas para el salto de acuerdo con el análisis del terreno; comandos de salto; procedimientos para la guía y capacidades de las aeronaves que se emplean para el salto militar en caída libre (SMCL); técnicas para fijar puntos de impacto o de salto; empaque y procedimientos

de inspección; procedimientos de emergencia para navegación nocturna; alistamiento de material para el empaque, el alistamiento de armas y la configuración de sistemas avanzados de orientación militar. Durante el entrenamiento de SMCL cada estudiante planea y ejecuta una operación nocturna en la que deben saltar armados, equipados y con equipo de oxígeno suplementario. Los alumnos de este entrenamiento son sometidos a exigentes evaluaciones en cada una de sus fases.

- b. *Special Forces Qualification Course (SFQC)*: el USAJFKSWCS ha entrenado a oficiales de grado capitán en el curso de calificación para integrar las FF. EE. y, mediante programas de intercambio y transferencia de conocimientos, nombrarlos como orgánicos dentro del selecto grupo de instructores que conforman la institución norteamericana. Este curso consiste en seis fases secuenciales de entrenamiento que diseñan y perfilan al hombre de las FF. EE.: 1) guerra no convencional; 2) comandante de pequeñas unidades; 3) especialistas o modelo ocupacional de FF. EE.; 4) guerra especial; 5) lenguas extranjeras, y 6) planeamiento estratégico y entrenamiento en SMCL. Los oficiales que participan en este entrenamiento se enfocan en el planeamiento y la resolución de cursos de acción relacionados con operaciones distintivas de las FF. EE.

Entrenamiento colectivo

Este entrenamiento integra todas las capacidades de las FF. EE. (acción directa, reconocimiento especial y contraterrorismo) que se contemplan en el ciclo anual de entrenamiento, los Planes de Instrucción y Capacitación (PIC) y los Planes de Instrucción y Entrenamiento (PIE), los cuales se desarrollan teniendo en cuenta las necesidades operacionales. Las tareas técnicas y tácticas se realizan de forma individual y colectiva en cada uno de los niveles, de acuerdo con la organización especial de la unidad que realiza las OO. EE., como se describe a continuación.

1. *Batallón de Entrenamiento de Comandos (BECOM)*: como unidad subordinada de la unidad operativa mayor de FF. EE., es el encargado de la formación individual y colectiva de las FF. EE.; desarrolla la doctrina y todo lo relacionado con entrenamientos individuales y colectivos; lleva a cabo y mantiene los programas de entrenamiento de FF. EE., y proporciona capacitación y educación individual de nivel básico y avanzado para las FF. EE. El BECOM entrena, educa, desarrolla y sostiene los niveles óptimos de preparación para las FF. EE. Además, es el encargado de proporcionar

a los regimientos de FF. EE. los oficiales, suboficiales y soldados profesionales que requieren: capacitados, altamente educados, innovadores y adaptables a los distintos ambientes en los cuales las FF. EE. ejecutan sus operaciones.

Infraestructura

En la justa medida en que la organización de FF. EE. fue creciendo en tamaño y capacidades, su ecosistema de planeación, preparación, alistamiento, concentración y revitalización en cuanto a infraestructura fue alcanzando entornos ágiles que permiten a los operadores especiales contar con los servicios que requieren para cumplir objetivos específicos.

Esta infraestructura moderna comprende instalaciones como el edificio inteligente del CCOES, el cual funciona como un centro integrador de capacidades, por ejemplo Inteligencia y OO. EE., sistemas de comando y control de última generación, las cuales permiten que las FF. EE. sostengan las rigurosas apreciaciones dinámicas que exigen sus misiones. Ya en el nivel táctico, se encuentra el complejo de OO. EE. denominado Odiseo, que se encuentra ubicado en el Centro Nacional de Entrenamiento (CENAE), en la meseta militar de Tolemaida, y el cual aloja dos de los tres regimientos de FF. EE. y otras unidades de apoyo. Actualmente, Odiseo se proyecta como un centro de excelencia para el entrenamiento de unidades de OO. EE. de carácter regional y es allí donde se preparan los equipos de élite que participan en las competencias regionales “Fuerzas Comando”, de las cuales Colombia ha sido campeona en once ocasiones.

Esta infraestructura permite otorgarle a la organización de FF. EE. los servicios necesarios en cuanto a revitalización, entrenamiento, descanso y alistamiento operacional para desarrollar efectivamente sus acciones militares.

El inicio del fin: el proceso de selección de blancos de las FF.EE. y su interoperabilidad

La construcción de una perspectiva sobre la interoperabilidad debe comenzar por definir el término, que, de acuerdo con los manuales de doctrina del Ejército Nacional, debe ser observable. Sobre su importancia en los manuales de las FF. EE., el *Manual Fundamental de Referencia del Ejército MFRE 3-37 Protección* advierte que “el fratricidio puede ser más frecuente durante operaciones conjuntas

y multinacionales, cuando los desafíos de las comunicaciones y de interoperabilidad no están completamente resueltos y claros” (Ejército Nacional, 2017d, p. 1-18).

Ahora bien, y aunque el *Manual de Términos y Símbolos del Ejército Nacional* define la interoperabilidad como la capacidad de operar en sinergia, cuando las unidades ejecutan tareas o misiones asignadas por un comando (Ejército Nacional, 2017b), para el presente ejercicio se propone la aproximación mucho más específica del *Diccionario de Términos y Símbolos* del Departamento de Defensa de los Estados Unidos:

[La interoperabilidad es la] habilidad para actuar en conjunto de manera coherente, efectiva y eficiente para alcanzar objetivos en el nivel táctico, operacional y estratégico. 2. Las condiciones alcanzadas entre sistemas de comunicación electrónica o artículos y equipos de comunicaciones cuando la información o los servicios pueden ser intercambiados directa y satisfactoriamente entre los usuarios. (Office of the Chairman of the Joint Chiefs of Staff, 2021, p. 110)

De acuerdo con Pablo Moreno (2014), en la guerra contemporánea, con las estructuras de comando y control actuales y las nuevas formas de amenaza de carácter global, resulta complicado imaginar operaciones puramente específicas terrestres, navales y aéreas empleando capacidades militares de modo independiente, y no como la naturaleza interdependiente de una operación de FF. EE. exige (Moreno, 2014). Probablemente, y como el conflicto ha demostrado, se han podido ejecutar operaciones de manera unilateral, pero el efecto deseado se puede maximizar cuando en la naturaleza conjunta del planeamiento se integran la interdependencia y la interoperabilidad, factores determinantes en el resultado de una estrategia que pueda ser eficiente y eficaz para el orfebre operacional.

Asimismo, esta cualidad le permite ejecutar operaciones de manera precisa, discreta y escalable dentro de cualquier operación mayor o campaña de acuerdo con los objetivos estratégicos y sus dos capacidades críticas: los ataques de precisión quirúrgica y la guerra especial (Ejército Nacional de Colombia, 2017a). Vale la pena precisar que el tiempo de respuesta y ejecución resulta de vital interés en el planeamiento de los cursos de acción para cumplir los objetivos de naturaleza estratégica. Estas cualidades han permitido a las Fuerzas de OO. EE. colombianas destacarse en ataques de precisión quirúrgica contra objetivos de carácter estratégico, entre los cuales se encuentran la neutralización de Walter Patricio Arizala, alias *Guacho*, en el departamento de Nariño en diciembre de 2018, así como la

operación contra alias *Fabián*, cabecilla del Frente de Guerra Occidental de la guerrilla del Ejército de Liberación Nacional (ELN), en septiembre del 2021.

La habilidad adquirida a través del desarrollo de actividades típicas de FF. EE. contra amenazas híbridas ha permitido desarrollar tácticas, técnicas y procedimientos (TTP) exclusivos de FF. EE. que han servido y seguirán siendo referencia para los estrategas militares de la organización de FF. EE. debido a la intrepidez y efectividad de los métodos únicos que emplean.

Para el doctor Tom Searle (2017), las OO. EE. son todas aquellas que se encuentran “fuera de la caja” de la naturaleza convencional de las operaciones militares. Searle (2017) plantea en su Teoría de Operaciones Especiales que estas no son de élite ni especializadas, sino que su cualidad especial significa “diferente”. Aunque en su teoría se refiere a capacidades y métodos de empleo únicos, también es pertinente hacer referencia al pensamiento creativo que permite resolver problemas desde perspectivas diferentes, “generando ideas nuevas y útiles, reevaluando y combinando ideas viejas para resolver problemas” (Ejército Nacional de Colombia, 2019, s.p.). Esta integración de fines, formas y medios empleada por los comandantes y su estado mayor está basada en la aplicación integral de sus habilidades, conocimiento y experiencia. Específicamente, este enfoque cognitivo se denomina *arte operacional* (ARTOP) de acuerdo con el *Manual de Técnicas del Ejército MTE 5-01 Metodología de Diseño del Ejército*.

La evolución que han tenido las FF. EE. en el arte operacional, apoyadas en su creatividad, criterio y juicio en el desarrollo de sus actividades, les ha permitido desempeñarse con contundencia en sus misiones y alcanzar con significativa eficiencia los objetivos de alta retribución que se les han impuesto.

El arte operacional no está relacionado directamente con un nivel de la guerra específico, sino que se puede dar tanto en el nivel táctico como en el estratégico. Además, compromete cuatro elementos esenciales: el tiempo, el espacio, el propósito y el método o la forma como se cumplirá el objetivo estratégico de manera parcial o total, de manera que el balance adecuado le permitirá al comandante retener, mantener y explotar la iniciativa de su acción táctica (Ejército Nacional de Colombia, 2019). En este sentido, a toda luz se puede manifestar que el arte operacional, el pensamiento crítico y pensar fuera de la caja son argumentos por fuerza multidimensionales e interdependientes que contribuyen y maximizan las capacidades de planeamiento y ejecución de operaciones de naturaleza “diferente”.

La evolución, la interoperabilidad y la naturaleza “diferente” (fuera de la caja) de las operaciones de FF. EE. han permitido concentrar estrategias que se han

adaptado al ambiente operacional ambiguo existente, lo cual ha sido posible gracias a la ejecución constante y consuetudinaria de conocimientos (arte) en la dinámica operacional. Esta particularidad les ha permitido a las FF. EE. maximizar los efectos de aplicar la experiencia a la ciencia y, en consecuencia, cumplir objetivos militares estratégicos que impactan positivamente la estrategia militar general (Centro de Doctrina Conjunta [CEDCO], 2018).

A su vez, esta dinámica permite a las FF. EE. mantener un nivel de desempeño eficiente en su entrenamiento, alistamiento e interoperabilidad. Para alcanzar estos altos estándares, las FF. EE. desarrollan planes y programas de entrenamiento de primera calidad, que se pueden evidenciar en el éxito que han alcanzado sus unidades en el desarrollo de operaciones. Por ejemplo, se puede mencionar la operación específica “Osiris”, que se realizó en octubre del año 2021 dentro de la campaña de OO. EE. “Agamenón” contra Darío Antonio Úsuga, alias *Otoniel*, máximo cabecilla del Grupo Armado Organizado-Clan del Golfo. Como mencionó el señor Presidente de Colombia en rueda de prensa en el Fuerte Militar de Tolemaida, esta operación es “el golpe más duro que se la ha propiciado al narcotráfico en el siglo XXI y solo es comparable con la caída de Pablo Escobar en los años 90” (CNN en Español, 2021).

Ahora bien, los comandantes que han ejecutado este tipo de misiones han comprendido el significado del concepto de *estrategia*: la ciencia y el arte de planear para cumplir objetivos de naturaleza estratégica, y que son determinados por los intereses nacionales, en búsqueda de afectar las amenazas nacionales de manera contundente. En relación con los objetivos político-estratégicos, el *Manual de Estrategia Militar General 3-34* establece que para cumplir los objetivos políticos se debe considerar una conducción estratégica nacional mediante “la utilización de los campos del poder” (CGFM, 1997). Esta conducción estratégica que establece metas, asignando fuerzas y recursos, resulta entonces en un panorama más amplio que el solo conocimiento que tiene el comandante sobre la doctrina y las capacidades de los hombres bajo su mando, pues abarca también la combinación del arte y la ciencia para contribuir al cumplimiento de los objetivos estratégicos (Ejército Nacional de Colombia, 2016a).

De acuerdo con el profesor Dale Eikmeier (2015), docente del U. S. Army Command and General Staff College en Fort Leavenworth, Kansas, se pueden considerar algunas diferencias entre la ciencia y el arte:

- Hay que considerar al arte de una manera subjetiva y la ciencia de una manera objetiva.

- El arte no es lineal y avanza de forma lateral; la ciencia es lineal y progresa en un paso a paso relacionándose de modo vertical.
- El arte se estudia de manera holística como un todo; la ciencia divide por partes el problema para poder enfrentarlo.
- Finalmente, el arte es el camino, “el viaje”, mientras que la ciencia es “el destino”.

De ahí que en la estrategia militar se combinan estos dos conceptos en diferentes proporciones, de modo que el éxito es determinar “cuándo actuar como un científico y cuándo actuar como un artista” (Eikmeier, 2015, s. p.).

Como indica el *MTE 5-0.1 Metodología de Diseño del Ejército: Arte y Diseño Operacional* (Ejército Nacional de Colombia, 2019), el arte operacional puede ser aplicado en todos los niveles de la guerra por los comandantes y su Estado Mayor. Ellos se manifiestan a través de planes y órdenes que describen cómo (formas) las fuerzas deben emplear sus capacidades (medios) para cumplir los objetivos que se les han impuesto, lo que denominan el estado final deseado, que trascendentalmente representa el éxito de la misión (Ejército Nacional de Colombia, 2019).

Ahora bien, a continuación se hace una aproximación a los conceptos que se emplean a menudo en las Operaciones de FF.EE. para ejecutar una misión. Además, se explora lo que el arte operacional describe como la *ciencia* y lo que expresaría el *científico*, si la analogía lo permite, es decir, el comandante en su planeamiento. Específicamente, estos conceptos tendrían la siguiente información:

El modo de la estrategia se refiere, por una parte, a que el comandante de unidad de FF. EE., como parte de una actividad típica dentro de sus capacidades, designa una operación y una tarea, y por otra, a la manera en que empleará las capacidades que tiene a su disposición para cumplir un objetivo estratégico específico. *Los medios* se refieren a las capacidades aéreas, navales y de infiltración especiales que el comandante solicita durante el planeamiento y que le son asignados luego de una evaluación. *El fin* consiste en el empleo de estas capacidades para lograr el estado final deseado, pero esta es la ciencia.

En este punto es importante destacar que para llegar a este concepto operacional, un *artista* ha tenido que evaluar múltiples cursos de acción dentro de su proceso militar para la toma de decisiones. Es decir, este comandante, junto con su Estado Mayor, ha descifrado una estrategia para cumplir un objetivo de carácter estratégico.

Acorde con este planteamiento, tal estrategia se podría expresar a través de una ecuación: Estrategia = Fines + Modos + Medios (Luttwak, 1989). Sin embargo,

de acuerdo con la literatura especializada, se deben tener en cuenta elementos adicionales, como el entorno y la estrategia del adversario, que sin duda alguna trascienden en el resultado de la ecuación (Álvarez et al., 2018).

Dentro del Rango de Operaciones Militares (ROM), las FF. EE. han evidenciado su habilidad para ejecutar acciones no solo a nivel de fuerzas conjuntas, sino también interagenciales, interorganizacionales y multinacionales, para una multiplicidad de misiones que van desde el entrenamiento a FF. EE. en naciones anfitrionas, hasta las operaciones de combate más importantes a nivel local.

Como se ha mostrado, las FF. EE. son una respuesta versátil y eficiente en cada punto del ROM, de manera que pueden proporcionar al Estado colombiano o a una nación anfitriona una serie de operaciones desplegables, ágiles, capaces de contribuir a esfuerzos conjuntos, para revertir rápidamente las condiciones de inestabilidad mediante la solución ética y decisiva de un conflicto. Pero estas respuestas siempre estarán condicionadas a ambientes operacionales inciertos, como lo describe la doctrina del Ejército Nacional con el término VICA (volátil, incierto, complejo y ambiguo). Esta estrategia, entonces, está condicionada a circunstancias cambiantes en un ambiente donde predominaría la suerte y la incertidumbre (Álvarez et al., 2018).

Ahora bien, en el contexto operacional de las OO. EE., un factor observable en los estrategias de la organización de FF. EE. es la intuición –no tanto la suerte–, que surge por el correcto entendimiento de las variables operacionales que afectan la misión. La adecuada lectura del ambiente operacional le permite al estratega darle enfoques dinámicos a una misión, llevar el *tempo* de la operación de forma consciente y responsable, pues sabe que su estimación de un indicio, un animal o una huella pueden representar el desenlace exitoso o no de una operación.

En general, el Ejército Nacional emplea cuatro actividades de carácter general en el proceso de operaciones: planear, preparar, ejecutar y evaluar, las cuales constituyen un común denominador en los tres métodos de planeamiento que, según la doctrina militar del Ejército Nacional, emplea la organización de FF. EE.: 1) la Metodología del Diseño del Ejército (MDE), 2) el Proceso Militar para la Toma de Decisiones (PMTD) y 3) el Procedimiento de Comando (PDC). Si bien estos métodos científicos se aplican en diferentes escalones, se encuentran alineados y contribuyen en últimas al mismo estado final deseado.

Uno de los factores que las FF. EE. evalúan constantemente dentro de sus capacidades distintivas son las metodologías del planeamiento. En ese

sentido, identificar las características del proceso de adquisición de blancos en las Operaciones de FF.EE. en un caso de estudio va más allá de lo que la ciencia dictamina, pues no es lineal. Para entender mejor este punto, se debe señalar que la interoperabilidad se ha construido en la justa medida en que la cultura organizacional de la institución identificó que “la ejecución” de este proceso es su valor agregado, pues allí se encuentra una de las características imprescindibles para lograr el éxito de sus misiones.

Este proceso de planeamiento se produce en el nivel operativo y es gestionado por el CCOES y la DIVFE. Si bien esta actividad se desarrolla en ese nivel superior, para que se materialice de forma efectiva debe estar estrechamente relacionada con la ejecución en el nivel táctico, de tal manera que su naturaleza interdependiente con los distintos niveles garantice el éxito de los objetivos estratégicos que establece la Estrategia Militar General. Por consiguiente, el CCOES y la DIVFE “construyen” las estrategias para alcanzar los blancos con base en lo que se considera una piedra angular: la “Integración Temprana”, definida como el resultado de un esfuerzo tridimensional donde se conjugan los análisis de las agencias de inteligencia y la visión prospectiva de especialistas en planeamiento y en operaciones para maximizar el resultado de la estrategia.

Siguiendo este proceso, las estrategias se traducen en cursos de acción que surgen en el TPOE. Esta afirmación se puede ejemplificar con la descripción que hizo el señor Comandante General de las Fuerzas Militares en la rueda de prensa después de la operación “Osiris”, en la cual fue neutralizado alias *Otoniel*, temido narcotraficante y máximo cabecilla del Clan del Golfo:

Esta operación definitiva contra este bandido fue planeada el 15 de octubre del 2021; se reúnen el Comandante General de las FF. MM. con oficiales de Inteligencia de la Policía Nacional, con oficiales de planeamiento de Operaciones Especiales y de la Policía, y se da un salto conceptual en el cambio de la estrategia empleada por las unidades para poder capturar a este bandido el 23 de octubre del año 2021. (Noticias Caracol, 2021, párr. 2)

Esta disposición de capacidades evidencia los primeros factores que se refieren al planeamiento conceptual:

1. Recepción de la información.
2. Análisis exhaustivo de esa información y de las variables operacionales.
3. Viabilidad de la operación.

4. Inicio del planeamiento conceptual y elaboración de conceptos operacionales que describan el propósito y los medios para alcanzar ese estado final deseado.
5. Aprobación por parte de los comandos superiores; en este estado se puede rediseñar la operación de acuerdo con las orientaciones que ellos emitan.
6. Entrega del concepto operacional e inicio del planeamiento militar para la toma de decisiones. Este proceso incluye la Integración Temprana y convoca a los comandantes de unidad operativa menor, denominados en el caso colombiano como Regimientos de Fuerzas Especiales. Si bien este hito determina el inicio de un paso, el “planeamiento paralelo” desarrollado por las unidades les permite adelantarse a eventos o ensayos, los cuales se deben prever antes de lanzar una operación debido a las condiciones de tiempo restringido en las que se efectúa este planeamiento.

Asimismo, se debe destacar que estos pasos también comprenden varios eventos dentro del proceso de selección de blancos y que son contemplados en el planeamiento conceptual: 1) aquel que orienta la guía inicial del comandante, 2) aquellos elementos que determinan el estado final deseado y 3) las líneas de esfuerzo que llevarán a cumplir la misión. En esta fase nace el centro de gravedad de la operación, que constituye el mecanismo de derrota que se va a emplear y que desencadena los elementos que focalizan el planeamiento detallado.

Estos aspectos se pueden evidenciar en la rueda de prensa que dio el Comandante General de las Fuerzas Militares sobre la operación “Júpiter” contra *Iván Mordisco*, en la cual resalta que,

[...] el señor Presidente de la República precisa una estrategia con líneas de acción como conjuntes en las capacidades de las FF. MM., incluyendo Inteligencia, apoyo interinstitucional con la Fiscalía y entrenamiento diferencial en unidades con capacidades de precisión quirúrgica. (Semana, 2022, párr. 3)

En esa oportunidad, el Comandante General de las Fuerzas Militares también describió algunos aspectos de las misiones que permiten configurar un ambiente operacional propicio para hacer frente a Grupos Armados Organizados. Específicamente, señaló que esta operación de configuración se realizó durante casi 24 meses, lo cual demuestra el nivel de participación de las FF. EE. en todo el rango de operaciones militares, es decir, lo que se denominaría una “Campaña de Operaciones Especiales”.

En la ejecución de la Operación de Fuerzas Especiales “Júpiter”, contra el terrorista *Iván Mordisco*, se pueden contar más de 288 días en empleo de capacidades diferenciales con Inteligencia dominante; la participación de más de 700 operadores especiales con un estricto comando y control; la evaluación de alrededor de 4 áreas nombradas de interés general y la realización de 12 eventos operacionales. De esta manera, el elevado nivel de búsqueda precisa y de perseverancia después de registrar 1900 km permitió localizarlo en un área de interés específica para realizar un ataque de precisión quirúrgica.

Esta operación, de carácter conjunto e interinstitucional, constituye una muestra de interoperabilidad e interdependencia, una actividad expresa de capacidades de análisis y ataque de la Fuerza Aérea, empleo del poder terrestre a través de unidades de FF. EE. e Inteligencia de la Policía Nacional, en la cual se emplearon varias plataformas de lanzamiento de operaciones y que tuvo como tarea clave conservar la legitimidad de la operación con la aplicación de los procedimientos jurídicos correspondientes.

Siguiendo con el análisis conceptual, el proceso de planeamiento, selección y priorización de blancos continúa de esta manera:

1. Concentración de medios técnicos, tecnológicos, aéreos y unidades de FF. EE. en lugares que permitan en tiempo, espacio y propósito cumplir la misión.
2. Planeamiento de unidades de maniobra basado en las variables de la misión.
3. Seguimiento a la batalla. Las apreciaciones dinámicas que se hacen en esta etapa permiten reevaluar en puntos decisivos de la misión las tácticas, las técnicas y los procedimientos que se deben emplear para continuar el esfuerzo operacional de forma adecuada.
4. Procedimientos jurídicos, vitales para garantizar la legitimidad de los procedimientos tácticos. Esta acción se realiza de manera paralela en todo el proceso de planeamiento, es coordinada desde el nivel operacional e influye directamente en la ejecución y posterior evaluación de la misión.
5. Extracción de unidades, bien sea para reubicarlas o para revitalizarlas y mantenerlas dispuestas operacionalmente para nuevas misiones.

Con base en lo anterior, la figura 3 sintetiza el proceso de planeamiento para seleccionar y priorizar los blancos de la organización de FF. EE. colombianas.

Figura 3. Proceso de planeamiento de las Fuerzas Especiales.



Nota: la elaboración invertida de la pirámide corresponde a un enunciado del profesor Humberto Serna Gómez, experto en planeación estratégica. El doctor Serna hace referencia al diseño de las estrategias de manera “top down” y a la ejecución de la estrategia de manera “bottom up” (Corporación Universitaria Minuto de Dios [UNIMINUTO], 2012).

Fuente: Elaboración propia con base en el Manual de Campaña del Ejército MCE 3-18 Operaciones de Fuerzas Especiales (Ejército Nacional de Colombia, 2018).

Ahora bien, el análisis efectivo sobre este proceso debe reunir unas características que trascienden la ciencia de la doctrina e incluir elementos “no tangibles” (UNIMINUTO, 2012), los cuales están relacionados estrictamente con cuatro aspectos relevantes de la definición de blancos:

1. La ejecución de la estrategia.
2. La credibilidad de los directivos de la organización, es decir, los comandantes, que, más allá de la estrategia, formulan y diseñan una prospectiva estratégica para anticiparse a la acción o a aquellas turbulencias que pudieran dictaminar las contingencias. Estos estrategas deben considerar unas categorías de la información que en el ámbito militar se denominan *variables operacionales* y *variables de la misión*, mediante las cuales pueden identificar los actores que las conforman para anticipar los riesgos de una operación.

3. La calidad de la estrategia planteada. Este aspecto está relacionado con la distinción que hace el Ejército Nacional entre metodologías de planeamiento, metodología de diseño, proceso militar para la toma de decisiones y procedimiento de comando, y, por último, el desarrollo de operaciones en el nivel táctico.

La importancia de incluir estos aspectos en el análisis radica en que “más del 60 % de una organización [está conformada por] aquellos elementos no tangibles, como los principios de una institución” (UNIMINUTO, 2012).

También se debe tener en cuenta que se pueden presentar dos tipos de ventajas: una comparativa, que dura hasta que otra organización la copia, y una competitiva, que consiste en una característica del proceso que le otorga una cadena de valor. Precisamente, el proceso de selección y priorización de blancos representa una ventaja competitiva en la cultura organizacional de las FF. EE., la cual está representada en su capital humano, “hombres culturalmente astutos, regionalmente alineados, políticamente matizados, entrenados en mediación y negociación, competentes en coordinación interorganizacional, maduros y que se espera operen de manera autónoma” (Ejército Nacional de Colombia, 2017a, s.p.). Ese es el *know how* que caracteriza el proceso de interoperabilidad.

Conclusiones

A toda luz, el presente trabajo académico no pretende enfatizar las propuestas organizacionales que se evidenciaron en la descripción contemporánea de la historia de las FF. EE. Si bien dicha evolución permitió crear una cultura estratégica que orienta las metodologías de planeamiento que emplean las FF. EE. con un enfoque determinado, se debe destacar que los resultados no son ambiguos ni se obtienen por azar, sino que se derivan de la sinergia e interdependencia que tienen las capacidades en el sistema.

Así, la investigación describe el proceso de adquisición de blancos en ataques de precisión quirúrgica desarrollados por las FF. EE. colombianas. Además, muestra cómo sus alcances y éxitos no constituyen el simple *output* de un ejercicio táctico, sino que se deben a un engranaje que amalgama una capacidad que se construyó de manera geoestratégica, la cual se explicó cuando se abordó el DOMPILEM. En este sentido, estos elementos no son por sí solos un factor de éxito, sino que participan en un proceso que requiere innovación y amplio entendimiento, de tal manera que esas “notas” fluyan como una sinfonía que desafía la

ambigüedad de las variables operacionales y que permite mantener el *tempo* de una operación.

En relación con el interrogante que derivó esta investigación sobre los procesos de selección de blancos de las FF. EE., se concluye que tienen una naturaleza interoperable, lo cual se puede ejemplificar en dos estudios de caso: la operación mayor "Agamenón" y la operación contra Walter Arizala, alias *Guacho*. Estas dos OO. EE. evidencian que el proceso tiene un alto nivel de interoperabilidad, pues en la primera campaña se emplearon elementos de la Policía Nacional, de Fuerzas convencionales y de FF. EE., mientras que la segunda misión involucró Fuerzas de países aliados (Colombia-Ecuador) para cumplir un objetivo común.

En este sentido, el estudio del proceso de selección de blancos de las FF. EE. permite hacer el siguiente diagnóstico. Con respecto a la interoperabilidad, la capacidad DOMPILEM se construyó alineada a intereses regionales y elementos empleados por países aliados como Estados Unidos. En efecto, el proceso que pueden emplear otras organizaciones para que sea exitoso debe tener en cuenta elementos que trascienden lo netamente material.

Lo anterior lleva a concluir que las características derivadas del proceso de selección y priorización de blancos son "no tangibles de la organización" y que están representadas en cuatro aspectos importantes para la planeación estratégica: 1) la ejecución de la estrategia, 2) la credibilidad de los directivos de la organización, 3) la calidad de la estrategia planteada, y 4) el desarrollo de las operaciones. Este proceso de selección empleado por las FF. EE., como menciona Serna (UNIMINUTO, 2012), es una ventaja competitiva para la organización de FF. EE., es difícilmente copiable, perdurable en el tiempo y genera el valor agregado para que sea considerado como una competencia distintiva del Ejército Nacional colombiano.

Referencias

- Álvarez, C., Corredor, C., & Vanegas, O. (2018). Pensamiento y cultura estratégica en seguridad y defensa: Bases para la construcción de una gran estrategia del Estado. En C. Álvarez & A. Fernández (Eds.), *La "Gran Estrategia": Instrumento para una política integral en seguridad y defensa* (pp. 15-63). Sello Editorial ESMIC. <https://doi.org/10.21830/9789585692862>
- Brigada de Fuerzas Especiales. (2015). *Historia y cultura militar del arma de Fuerzas Especiales*. Publicaciones Internas.
- Castaño, C., & Arias, J. (2015). Aproximación a la valoración del know how de una institución del sistema regional de innovación en Antioquia. *Revista Civilizar Ciencias Sociales y Humanas*, 15(28), 151-164. <https://tinyurl.com/2kdzkej>
- Centro de Doctrina Conjunta [CEDCO]. (2018). *Manual Fundamental Conjunto MFC 1-0 [Público]*. Publicaciones Comando General de las Fuerzas Militares de Colombia. <https://doi.org/10.25062/MFC10>
- CNN en Español. (2021, 23 de octubre). Iván Duque: captura de alias "Otoniel" es comparable con la de Pablo Escobar [Video]. YouTube. <https://www.youtube.com/watch?v=9h-PiTwhuNwY>
- Comando Conjunto de Operaciones Especiales [CCOES]. (2014). *Libro Estructural Comité de Revisión Estratégica del Comando Conjunto de Operaciones Especiales CCOES*. Comando General de las Fuerzas Militares Colombia.
- Comando General de las Fuerzas Militares [CGFM]. (1997). *Manual de Estrategia Militar General* (2.a ed.). Publicaciones de las Fuerzas Militares.
- Corporación Universitaria Minuto de Dios [UNIMINUTO]. (2012, 19 de junio). Planeación estratégica: doctor Humberto Serna Gómez [Video]. YouTube. <https://www.youtube.com/watch?v=WqfFwYQaiow>
- Eikmeier, D. (2015, 13 de octubre). Operational art, design and the center of gravity [Video]. YouTube. <https://www.youtube.com/watch?v=nBStKk3fE4E>
- Ejército Nacional de Colombia. (2016a). *Manual Fundamental del Ejército MFE 1-01 Doctrina [Público]*. Imprenta Militar del Ejército. <https://tinyurl.com/h8ywavpv>
- Ejército Nacional de Colombia. (2016b). *Manual Fundamental del Ejército MFE 3-90 Operaciones Ofensivas y Defensivas [Público]*. Imprenta Ejército. <https://tinyurl.com/2w7zdbzm>
- Ejército Nacional de Colombia. (2016c). *Manual Fundamental del Ejército MFE 5-0 Proceso de Operaciones [Público]*. Imprenta Militar del Ejército. <https://tinyurl.com/2t56cvyx>
- Ejército Nacional de Colombia. (2017a). *Manual Fundamental del Ejército MFE 3-05 Operaciones Especiales [Público]*. Imprenta Militar del Ejército. <https://tinyurl.com/2p8b7nse>
- Ejército Nacional de Colombia. (2017b). *Manual Fundamental de Referencia del Ejército MFRE 1-02 Términos y Símbolos [Público]*. Imprenta Ejército. <https://tinyurl.com/3byekp57>
- Ejército Nacional de Colombia. (2017c). *Manual Fundamental de Referencia del Ejército MFRE 3-0 Operaciones. [Público]*. Imprenta Ejército. <https://tinyurl.com/duc7tje>

- Ejército Nacional de Colombia. (2017d). *Manual Fundamental de Referencia del Ejército MFRE 3-37 Protección [Público]*. Imprenta Ejército. <https://tinyurl.com/4pved58t>
- Ejército Nacional de Colombia. (2018). *Manual de Campaña del Ejército MCE 3-18 Operaciones de Fuerzas Especiales [Restringido]*. Imprenta Ejército.
- Ejército Nacional de Colombia. (2019). *Manual de Técnicas del Ejército MTE 5-0.1 Metodología de Diseño del Ejército [Público]*. Imprenta Ejército. <https://tinyurl.com/3zjfspr2>
- Ejército Nacional de Colombia. (2023, 2 de noviembre). Organigrama. <https://tinyurl.com/bddtmw64>
- Gallardo, M., & Faundes, C. (2014). ¿Qué es el pensamiento estratégico? *Escenarios Actuales*, 19(3), 7-23. <https://tinyurl.com/56jmk66j>
- Luttwak, E. (1989). *Estrategia: La lógica de guerra y paz*. Instituto de Publicaciones Navales.
- Martínez Carazo, P. C. (2006). El método de estudio de caso: Estrategia metodológica de la investigación científica. *Pensamiento & Gestión*, (20), 165-193. <https://tinyurl.com/5hd4xftn>
- Ministerio de Defensa Nacional [MDN]. (2016). *Visión futura de las Fuerzas Armadas*. Imprenta Nacional de Colombia. <https://tinyurl.com/bdzfy898>
- Ministerio de Defensa Nacional [MDN]. (2019). *Política de Defensa y Seguridad PDS: Para la legalidad, el emprendimiento y la equidad*. Ministerio de Defensa Nacional. <https://tinyurl.com/5n98jdwf>
- Montero, L., Garzón, O., Quevedo, O., Tobón, A., & Player, N. (2019). Relevancia estratégica de las Operaciones Especiales: Lecciones de la experiencia colombiana. En L. Montero (Ed.), *El poder terrestre: Ejércitos y guerras del siglo XXI* (pp. 173-199). Escuela Superior de Guerra. <https://doi.org/10.25062/9789585698369>
- Moreno Delgado, P. (2014). *Poder y capacidad: El ocaso de los poderes* [Documento opinión, n.º 93]. Instituto Español de Estudios Estratégicos. <https://tinyurl.com/y2zuy6ct>
- Muñoz, L., & Cano, D. (2020). Evolución histórica de las Fuerzas Especiales en Colombia. En J. Valdés & A. Rodríguez (Eds.), *Memorias imborrables: Guardias de honor* (pp. 61-90). Planeta. <https://doi.org/10.25062/9789584289001>
- Noticias Caracol. (2021, 23 de octubre). Así fue la intensa cacería a alias 'Otoniel', máximo cabecilla del Clan del Golfo [Video]. YouTube. <https://www.youtube.com/watch?v=Uf-kEGC1dJIA&t=156s>
- Office of the Chairman of the Joint Chiefs of Staff. (2021). *DOD Dictionary of Military and Associated Terms [Public]*. The Joint Staff. <https://tinyurl.com/rdekurva>
- Rojas, P. (2017). Doctrina Damasco: Eje articulador de la segunda gran reforma del Ejército Nacional de Colombia. *Revista Científica General José María Córdova*, 15(19), 95-119. <http://dx.doi.org/10.21830/19006586.78>
- Searle, T. (2017). *Outside the box: Special Operations theory* [JSOU Report, n.º 174]. The JSOU Press. <https://tinyurl.com/mr6hwc9y>
- Semana. (2022, 26 de julio). Alias "Iván Mordisco", su estructura armada disidente de las FARC y sus planes criminales. <https://tinyurl.com/3brbchk9>

Capítulo 3

Análisis prospectivo de las Operaciones de Fuerzas Especiales en megaciudades: Colombia y Brasil^{*}

DOI: <https://doi.org/10.25062/9786287602809.03>

Álvaro Iván Torres Cabra

Escuela Superior de Guerra "General Rafael Reyes Prieto"

Guilherme Lopes da Cunha

Escuela Superior de Guerra de Brasil ESG

Resumen: Nuevas amenazas en ambientes urbanos se destacan como uno de los desafíos significativos para los Estados. Hacer frente a la mutación de las amenazas implica combinar diferentes métodos y medios, en especial, cuando el crecimiento o la conurbación de áreas urbanas pueden derivar en una megaciudad. Grandes concentraciones de habitantes originan un potencial de disputas que pueden resultar en conflictos internos. Este estudio hace un análisis empírico que compara los centros urbanos de Río de Janeiro y Bogotá, D. C. Se utilizan metodologías cualitativas y cuantitativas: una propuesta analítica, una explicativa y un análisis de caso. La investigación plantea una mirada prospectiva de las Fuerzas Especiales en la que se consideran aspectos como el diseño operacional, la determinación de los centros de gravedad de amenaza, la doctrina de las Fuerzas Especiales en megaciudades y los alcances operacionales y estratégicos en conflictos de megaciudades.

Palabras clave: conflicto urbano; estrategia; Fuerzas Especiales; megaciudad; urbanización.

^{*} Este capítulo es resultado de investigación adscrito al proyecto "Naturaleza de la guerra contemporánea. Retos y oportunidades de las Fuerzas Especiales y la Inteligencia", adscrito al Departamento Ejército de la Escuela Superior de Guerra, inscrito en la línea de investigación "Naturaleza de la guerra, terrorismo, nuevas amenazas", que forma parte del grupo de investigación Centro de Gravedad, categorizado en A por Minciencias, con código COL0104976. Los puntos de vista pertenecen a los autores y no reflejan necesariamente los de las instituciones participantes.

Álvaro Iván Torres Cabra

Teniente Coronel del Ejército Nacional de Colombia. Magíster en Seguridad y Defensa Nacionales, Escuela Superior de Guerra "General Rafael Reyes Prieto", Colombia. Especialista en Administración de Recursos Militares para la Defensa Nacional, Escuela de Logística del Ejército. Profesional en Ciencias Militares, Escuela Militar "General José María Córdova", Colombia. Administrador de la Seguridad y Salud Ocupacional, Universidad Militar Nueva Granada, Colombia. Contacto: alvaro.torresca@buzonejercito.com.co

Guilherme Lopes da Cunha

Candidato a Posdoctor en Relaciones Internacionales, Universidad de Brasília. Doctor y magíster en Economía Política Internacional, Universidad Federal de Río de Janeiro. Profesor de la Escuela Superior de Guerra del Ministério de Defesa de Brasil.

<https://orcid.org/0000-0002-8639-747X> - Contacto: guilherme.lopes@esg.br

Citación APA: Torres Cabra, A. I., & Lopes da Cunha, G.(2024). Análisis prospectivo de las Operaciones de Fuerzas Especiales en megaciudades: Colombia y Brasil. En L. A. Montero Moncada & O. A. Garzón Gómez (Eds.), *Comandos: Retos de las Fuerzas Especiales e Inteligencia en la guerra contemporánea* (pp. 65-92). Sello Editorial ESDEG. <https://doi.org/10.25062/9786287602809.03>

COMANDOS: RETOS DE LAS FUERZAS ESPECIALES E INTELIGENCIA EN LA GUERRA CONTEMPORÁNEA

ISBN impreso: 978-628-7602-79-3

ISBN digital: 978-628-7602-80-9

DOI: <https://doi.org/10.25062/9786287602809>

Colección Seguridad y Defensa

Sello Editorial ESDEG

Escuela Superior de Guerra "General Rafael Reyes Prieto"

Bogotá D.C., Colombia

2024



Introducción

La guerra urbana no es un fenómeno nuevo. Las ciudades se han presentado como un escenario para la violencia desde que los seres humanos comenzaron a construirlas. La disparidad de la riqueza ha conducido a la conformación de ecosistemas criminales urbanos (término que resulta conveniente para examinar la correlación entre grupos al margen de la ley y el entorno geográfico).

Lo anterior permite hacer una observación del ecosistema criminal urbano y determinar cuál es el escenario en el cual se articulan los grupos al margen de la ley, la población civil y otros actores interdependientes. Usualmente, los ecosistemas criminales se encuentran localizados en los barrios marginales, en cinturones de miseria o en zonas de tolerancia. Las historias de Alepo, Mosul, Marawi, Mogadishu, Donetsk y Mekelle se pueden tomar como ejemplo, debido a que ratifican que tanto los pueblos como las ciudades serán objetivos militares estratégicos futuros.

El crecimiento poblacional no planeado y desorganizado de las áreas urbanas en las principales ciudades del mundo avanza de forma apresurada. Algunos estudios proveen datos alarmantes proyectados para el 2050 que indican cuáles centros urbanos enfrentarán desafíos más complejos en temas de seguridad y defensa (Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura [UNESCO], 2017).

Si a esto se suma la búsqueda de una mejora en la calidad de vida, se refuerza el valor estratégico de las ciudades y se evidencia que se convierten en núcleos vitales de las naciones. Por consiguiente, la singularidad física del terreno y la presencia de un gran número de población incrementan considerablemente la complejidad en relación con los riesgos colaterales durante la conducción de operaciones en ambientes urbanos.

Las megaciudades son un escenario difícil de predecir, puesto que requieren la conducción de operaciones conjuntas, coordinadas, interinstitucionales y multilaterales (CCIM), que permitan contrarrestar el crimen organizado transnacional (COT). Cabe señalar que esta es la base fundamental de la doctrina asumida por el señor Comandante General del Ejército Nacional para afrontar los desafíos actuales (Escuela Superior de Guerra [ESDEG], 2021). En ese orden, se tiene como escenario un ambiente operacional volátil, incierto, complejo y ambiguo (VICA), que caracteriza la naturaleza de algunas condiciones y situaciones difíciles (Wigmore, 2017).

Otra ventaja para la amenaza es el empleo de las tecnologías de la información, dado que estas potencian los estereotipos de conducta, los cuales han añadido una capa adicional de dificultad en los espacios de conflictos tradicionales y, como resultado, han cambiado su dinámica habitual. El acceso global al entorno virtual ha creado oportunidades incontables para propiciar conflictos en línea que afecten dominios virtuales (sistemas informáticos), dominios cognitivos (actitudes, conocimientos y creencias de las personas) y dominios físicos. En consecuencia, esto significa que la guerra ya no se limitaría a los adversarios armados, sino que se expandiría para abarcar todos los aspectos de la experiencia humana (Álvarez et al., 2018).

Con base en lo anterior, este documento investigativo hace un análisis prospectivo de las Operaciones de Fuerzas Especiales (FF. EE.) en Bogotá, D. C., y Río de Janeiro, dos ciudades latinoamericanas que no son ajenas a la evolución de la globalización desviada¹ y que reflejan su “lado oscuro”: la proliferación del comercio ilícito (posibilitado por los mismos medios tecnológicos) y la prosperidad de la globalización lícita (que ha incrementado la movilidad global) (Zambrano & Álvarez, 2017).

Adicionalmente, el estudio de los desafíos que enfrentan las FF. EE. de Estados latinoamericanos en este escenario permite proponer la hipótesis relacional de que el surgimiento de las megaciudades implica un mayor potencial de conflictos y, a su vez, la necesidad de mejorar los aparatos estatales de seguridad para mantener la seguridad de personas e instituciones. En ese sentido, se formulan las siguientes preguntas: ¿Cuáles son las implicaciones para las Operaciones de las FF. EE. en megaciudades como escenario de conflicto? ¿Cómo contribuye una comparación de otras experiencias (como las que ocurren entre Río de Janeiro y Bogotá, D. C.) a investigar el fenómeno de conflicto urbano en futuras megaciudades suramericanas?

¹ Es decir, aquella en la cual se usan las manos fraudulentas a fin de generar todo tipo de delitos sacando provecho de las bondades de la tecnología.

Este capítulo está compuesto por tres temas principales. El primero es la investigación sobre la naturaleza de los conflictos urbanos y del escenario de intensificación demográfica, aspectos que inducen a reflexionar acerca de los desafíos de contención de amenazas multidimensionales. El segundo es la búsqueda de respuestas político-estratégicas asociadas a la capacidad de adaptación táctica-operacional que tienen las FF. EE. para lidiar con el panorama identificado en la primera parte. El tercero es la propuesta de un estudio de caso en el que se comparan Río de Janeiro y Bogotá, D. C. Los resultados de la investigación evidencian diferencias y similitudes entre Brasil y Colombia que permiten identificar la necesidad de modernizar de forma constante los mecanismos que garantizan la neutralización y supresión de amenazas en un ambiente urbano.

La formación de megaciudades y los escenarios de conflicto

La urbanización está en una expansión continua que depende de la conectividad para integrar el transporte, la energía y la comunicación, factores que le permiten generar un salto cuantitativo en la movilidad de las personas, bienes, recursos y conocimientos, a fin de conformar la civilización de red global del siglo XXI. Como parte de la urbanización planetaria, en el 2030 más de dos tercios de la población mundial vivirá en ciudades y, además, se tendrán cincuenta grupos de megaciudades (dentro de las cuales se encuentran Río de Janeiro y Bogotá, D. C.) en un ambiente en que las ciudades quieren ser parte de la cadena de valor global (Khanna, 2016a).

En *"Architecture, Globalization and Identity"*, King (2008) explica las tendencias importantes y observables que presagian el futuro de la guerra. Por ejemplo, señala que las ciudades siempre han sido lugares de encuentro en donde se intercambian bienes y servicios, y que sus habitantes reciben protección a cambio de una subordinación a un poder político. Además, agrega que existen diversos factores que alimentan el dinamismo de la transición urbana: por un lado, las personas sienten la presión de emigrar del campo para escapar de la pobreza y de las amenazas a su seguridad; por el otro, lo hacen al estar atraídos por una ciudad que promete un modo de vida más completo e interconectado con la globalización.

De manera complementaria, evidencias estadísticas señalan un futuro desafiante para el ambiente urbano. La expansión demográfica en las ciudades y los cambios que resultan de esa reconstrucción del espacio crean un contexto de

incertidumbre, el cual subraya la necesidad de establecer planes efectivos para gestionar mecanismos de seguridad. Según la Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura (UNESCO, 2017), los centros urbanos pasarán por una transformación desafiante:

Por primera vez en la historia, más personas viven en áreas urbanas que rurales, una proporción que se espera que aumente para el año 2050. Con las ciudades creciendo verticalmente y las poblaciones cada vez más densas, los centros urbanos se volverán cada vez más congestionados, complejos e interdependientes (p. 22).

El informe de la UNESCO (2017) apunta a una realidad que tendrá impactos significativos en la seguridad del sistema internacional. Conscientes de esas condiciones, miembros de la Organización de las Naciones Unidas (ONU) proponen líneas de acción que detallan los análisis que hace su Departamento de Asuntos Económicos y Sociales.

Así, se evidencia que el escenario de conflicto se ha trasladado al ámbito urbano, el cual está compuesto por una gama amplia de estructuras sociales en un espacio determinado. Para ayudar a contextualizar el objetivo de la investigación, se debe señalar que los términos *ciudad* y *urbano* se suelen utilizar como sinónimos, pero pueden denotar conceptos diferentes:

Ciudad se refiere a la agrupación estadística de personas en una sola área y *urbano* se refiere a la transformación en la mentalidad que se produce en las ciudades; en otras palabras, el concepto de lo urbano denota generalmente los patrones alterados de interacción social, económica, política y cultural. (Comisión Económica para América Latina y el Caribe [CEPAL], 1989, p. 72)

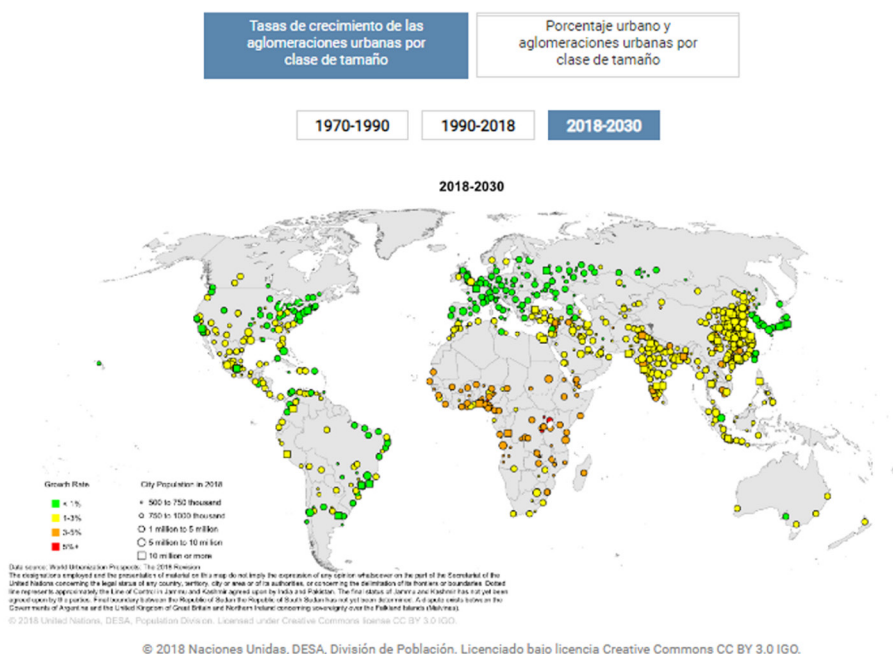
Como se verá más adelante, estas características hacen necesario estudiar una diversidad de variables para generar doctrina.

Ahora bien, el crecimiento de las ciudades representa un desafío para la gestión pública en el presente y en el futuro. Algunas características sobresalen en las reflexiones acerca de las ciudades, como la expansión demográfica, el desorden en la lógica de ampliación, la conurbación, entre otros elementos. En ese proceso, la comunidad internacional presenta opciones políticas, como la propuesta de la Nueva Agenda Urbana (Urban Agenda Platform, 2022), que fue adoptada en la ONU por la Conferencia de las Naciones Unidas sobre Vivienda y Desarrollo Urbano Sostenible (Hábitat III) en Quito, Ecuador, el 20 de octubre de 2016.

En ese contexto, se ha dado la movilización de miembros de la entidad y otros actores para implementar el desarrollo urbano a nivel local. De hecho, por medio de la Resolución N.º 70/1 de la Asamblea General de las Naciones Unidas (25 de septiembre de 2015), se crearon 17 Objetivos de Desarrollo Sostenible (ODS), uno de los cuales, el número 11, pretende velar por que se generen ciudades inclusivas, seguras, resilientes y sostenibles (ONU, 2015).

No obstante, los datos ofrecidos por diversos órganos internacionales generan una preocupación desde la perspectiva multilateral. Por ejemplo, el Departamento de Economía y Asuntos Sociales de las Naciones Unidas publicó un estudio sobre el crecimiento de índices de aglomeración urbana (ONU, 2018a), cuyo pronóstico con respecto a las tasas de crecimiento urbano para los próximos años es alarmante (figura 1).

Figura 1. Tasa de crecimiento de aglomeración urbana (2018-2030).

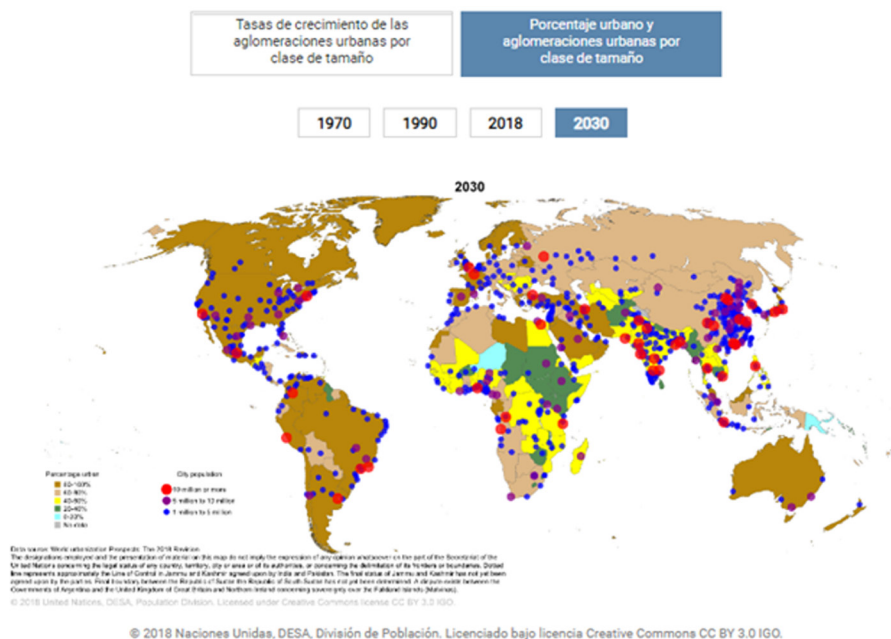


Fuente: ONU (2018d).

Los pronósticos apuntan a la ampliación de las tasas de crecimiento urbano en los próximos años (figura 2). Las estadísticas muestran datos relevantes para Suramérica, pero menos alarmantes que para otras regiones del mundo, hecho

que Milton Santos (2004) conceptúa como “macrocefalia urbana”. Sin embargo, las expectativas de aglomeración urbana constituyen un escenario de incertidumbre en ciudades con alta concentración demográfica.

Figura 2. Porcentaje urbano y aglomeraciones urbanas para el 2030.



Fuente: ONU (2018c)

Según las Naciones Unidas (2018d), una megaciudad se define como una ciudad con más de diez millones de habitantes. Hoy existen 24 megaciudades y se estima que, al menos, 27 ciudades serán clasificadas así en el 2025. Además, se proyecta que 752 millones de personas vivirán en megaciudades en el 2030, es decir, el 8,8 % de la población mundial.

Con base en lo anterior, se puede afirmar que las megaciudades y las áreas metropolitanas son un elemento clave de la reconfiguración geopolítica a escala global. De acuerdo con Iberdrola (2020), la megaciudad más grande en la actualidad es Tokio, Japón, puesto que tiene una población de más de 32 millones de habitantes en un área demasiado pequeña para albergarlos.

Otra característica de las megaciudades, especialmente en aquellas del tercer mundo, es que están relacionadas con los altos índices de pobreza, la descomposición social, el mantenimiento de la infraestructura, las falencias en los servicios

básicos, las tasas de natalidad muy altas, las pocas oportunidades laborales, la transmisión de enfermedades, entre otras.

Con respecto a los Estados modernos, existe la preocupación por una situación en las grandes ciudades que devela el aumento de la criminalidad en distintas modalidades. El crecimiento de las áreas urbanas y las diferentes actividades ilícitas permiten a los grupos criminales enquistarse en los sectores menos favorecidos y convertirse en un desafío para la seguridad y la defensa nacionales (SDN). El concepto de "rinoceronte gris" (Izquierdo, 2018; Wucker, 2016) sirve para señalar que el problema es visible desde lejos, pero no se toman las medidas necesarias para contener la amenaza futura.

Conflictos urbanos entre Estados y/o intraestatales

En el siglo XXI, la prioridad de la humanidad es poder formar una urbanización sostenible, para lo cual es necesaria la tecnología, los conocimientos y las políticas públicas. Sin embargo, la desigualdad en distintos aspectos genera fricciones entre la población y, muchas veces, desencadena conflictos.

A pesar de ser un fenómeno antiguo, la naturaleza de los conflictos necesita ser diferenciada. Por una parte, está el tipo de combate ocasionado por un conflicto entre Estados, cuya guerra puede ocurrir en un área urbana; por la otra está el conflicto urbano, en el cual un Estado debe entrar en conflicto contra sus propios ciudadanos, lo que se conceptúa como "no guerra" (Alves, 2018).

Aun cuando los conflictos entre Estados deben ser objeto de análisis constante, el eje principal de la investigación que plantea este documento es verificar los conflictos intraestatales (uno de los grandes desafíos de Latinoamérica). No obstante, se considera que es importante evaluar primero las singularidades que tiene la actuación de las Fuerzas Militares en el ambiente urbano.

Las operaciones militares tienen múltiples tipos de riesgos implícitos, como los tácticos (que incluyen la posibilidad de que los soldados se lesionen o mueran, o que se incumpla la misión) y los accidentales (que incluyen la posibilidad de que los civiles mueran o que se destruya infraestructura urbana crítica). Estos factores deben ser considerados durante el planeamiento, con la intención de estudiar sus posibles implicaciones e instruir a las unidades en lo que respecta a los marcos legales.

En este sentido, una visión prospectiva de las operaciones que realizan las FF. EE. debe tener presente no solo que la urbanización es una tendencia implacable, sino que a medida que las ciudades crecen y se expanden, los conflictos armados y la violencia también se urbanizan (Lehmann, 2015). Esto ha sido evidente en ciudades como Alepo en Siria, Sana'a en Yemen y Mosul en el norte de Irak, que han sufrido guerras de asedio, bombardeos aéreos y de artillería, así como fuertes combates en las calles (Espinosa, 2017).

Con base en un análisis detallado de las batallas urbanas recientes y sus antecedentes históricos, King (2008) afirma que la exploración de la topografía cambiante y las tácticas en evolución del paisaje del conflicto urbano evidencian que las operaciones en las ciudades de hoy se han vuelto distintivas. Esto no significa que todos los métodos utilizados en la guerra urbana sean nuevos, sino que esta se ha transformado en microasedios extenuantes protagonizados por combatientes que luchan a través de edificios, calles y distritos individuales.

Implicaciones para las operaciones de Fuerzas Especiales

La incertidumbre y las complejidades en el ambiente urbano demuestran los desafíos presentes y futuros que tienen las Fuerzas Armadas. Frente a esto, se propone investigar los tres ejes principales de modernización de las FF. EE.: 1) los nuevos requerimientos en cuanto al diseño operacional y la determinación de centros de gravedad; 2) la doctrina de las FF. EE. en megaciudades, y 3) los alcances operacionales y estratégicos de las FF. EE. en conflictos en megaciudades. Estos elementos develan retos comunes que pueden ser verificados.

Nuevos requerimientos al diseño operacional y la determinación de centros de gravedad

Los centros urbanos presentan retos a una escala y complejidad superiores, dado que contienen territorios estratégicos que están interconectados con centros de gravedad locales, nacionales y, en algunos casos, internacionales. Independientemente de que se haya abordado desde hace varias décadas, el concepto "centro de gravedad" es fundamental en los conflictos actuales y se debe calibrar su utilización en contextos sociales e históricos diferentes (Cazumba, 2021).

Los responsables de planear las operaciones urbanas necesitan herramientas que los ayuden a darle sentido a un ambiente complejo de confrontación y a desarrollar un nivel aceptable de conciencia situacional, indispensable a fin de separar lo relevante de lo irrelevante, lo central de lo periférico. Luego, la importancia del centro de gravedad en el planeamiento militar se ve plasmada en cuatro criterios: mejorar el entendimiento, enfatizar el planeamiento, potenciar la eficiencia y eliminar la distracción.

El ambiente urbano posee cualidades únicas. Está conformado por espacios tridimensionales desordenados que presentan desafíos logísticos y de navegación relevantes. Su terreno, creado por el hombre, está compuesto por formas angulares que raramente ocurren en terrenos no urbanos: un patrón planimétrico y una tercera dimensión, cuya verticalidad es clave porque crea barreras bastante difíciles para el asalto y proporciona a la defensa otra forma artificial de altura, planos de suelo urbano alto y, en muchos casos, un nivel subterráneo.

Ahora bien, en el caso particular de Latinoamérica destaca la violencia urbana, alimentada por el COT. Parte de su formación consiste en alianzas con diferentes grupos armados, lo cual no solo produce una convergencia criminal entre insurgentes y grupos criminales, sino que además genera una red que comparte los mismos intereses y que se amplía a diferentes países.

Algunos ejemplos que se pueden mencionar son México y Brasil, que tienen unas de las tasas de homicidio más altas del mundo (Morán, 2021). También se debe mencionar que en Colombia hay múltiples ciudades, entre intermedias y grandes, que son epicentro de conflictos urbanos originados por el COT para mantener el dominio y la supremacía en el negocio de microtráfico. Este delito, eventualmente, se conecta con otros y ha ido desplazando a los carteles de drogas de las décadas de los años 80 y 90, cuya forma de operar era muy diferente.

En este contexto, la criticidad de las operaciones urbanas demanda una fuerza estructurada con capacidades y habilidades óptimas para enfrentar la amenaza. Al respecto cabe recordar dos hechos de importancia sucedidos en Colombia: el primero es la toma de la embajada de la República Dominicana en 1979, en Bogotá, D. C.. En esa época no se contaba con una unidad entrenada y experimentada que pudiera rescatar a los rehenes, lo cual obligó a descartar una operación militar y llevó a una mediación por parte de Cuba. El segundo es la toma guerrillera del Palacio de Justicia en 1985 por parte del grupo autodenominado Movimiento 19 de Abril (M-19), también en Bogotá, D. C., hecho que tuvo consecuencias desastrosas para la sociedad colombiana y de las cuales no se ha podido recuperar.

Acciones como estas, ocurridas en áreas urbanas, hicieron que fuera necesario contar con unas Fuerzas Militares entrenadas, equipadas y certificadas, a fin de prevenir, detener o proveer una respuesta efectiva. En consecuencia, mediante la Resolución Ministerial N.º 2270 del 30 de abril de 1986, se creó la Agrupación de Fuerzas Especiales Antiterroristas Urbanas (AFEAU), con el propósito específico de disponer de una unidad con capacidad para manejar situaciones de crisis y toma de rehenes en áreas urbanas, cuando se afecten gravemente los intereses de la nación (Valdés & Rodríguez, 2020). A la fecha, esta unidad ha sido entrenada, capacitada y certificada en técnicas, tácticas y procedimientos en ambientes urbanos, con misiones específicas para el manejo de situaciones de crisis.

Es importante mencionar que, dentro de la Tabla de Organización y Equipo (TOE) de las Fuerzas Militares, la AFEAU forma parte del Comando Conjunto de Operaciones Especiales (CCOES) (Comando General de las Fuerzas Militares [CGFM], 2016), unidad que representa un tridente estratégico basado en la conjunción de capacidades, el entrenamiento y la interoperabilidad para combatir a un adversario completamente amorfo e irregular.

Por su parte, el Ministerio de Defensa Nacional (MDN) ha apropiado la idea del combate urbano como una necesidad perentoria para hacer frente al terrorismo de los Grupos Armados Organizados (GAO), los cuales han amenazado la seguridad y defensa nacionales del territorio colombiano.

Doctrina de las F.F.EE. en megaciudades: estudio de caso y lecciones aprendidas

A lo largo del tiempo, los teóricos militares han reconocido que la defensa es la posición táctica más fuerte. De hecho, se necesita una mayor fuerza para atacar y derrotar a un enemigo que está en una defensa establecida y construida debidamente, que uno que se encuentre al aire libre. Esto es aún más cierto en el terreno urbano, por cuanto muchas de sus estructuras físicas ofrecen posiciones defensivas inmediatas de calidad militar para el defensor.

Por lo general, la mayoría de los ciudadanos adoptan una posición en medio del conflicto, la cual se basa en su capacidad de actuar, limitar, bloquear o desplazar algún tipo de operación urbana que se esté desarrollando. Por ejemplo, John Spencer (2022), quien se enfoca en los estudios de guerra urbana en el Instituto de Guerra Moderna (West Point), publicó el 26 de febrero de 2022 una serie de mensajes en la plataforma Twitter, hoy X, dirigidos a los resistentes civiles en Ucrania, particularmente en la capital del país, Kiev, cuya población aproximada es de tres

millones de habitantes. Este profesor cree que si los adultos de la capital se movilizan y hacen que las fuerzas rusas teman que un arma pueda estar apuntando por cada ventana y que cada calle sea una trampa mortal, podrían convertir a Kiev o a las otras ciudades en “puercoespines enormes” que pueden enfrentar con éxito a cualquier soldado, sin importar cuán avanzado sea (Spencer, 2022).

Sobre este ejemplo también se debe señalar que el dominio físico es un concepto preponderante en el conflicto ruso-ucraniano porque cualquiera de los dos bandos puede usarlo. Básicamente, las ruinas de los edificios antiguos y las zonas céntricas o comerciales pueden ser empleadas por fuerzas comprometidas que, sin duda alguna, les garantizarán una protección adecuada, puesto que el terreno urbano proporciona una ventaja significativa a la fuerza defensora, incluso a la más débil. Por lo tanto, evaluar la dificultad de la guerra en un ambiente específico requiere considerar al escenario mismo como una de las capacidades militares disponibles para cumplir la misión.

Otro de los conflictos que sirve como referente del empleo de las Fuerzas Especiales Urbanas tuvo lugar en Mosul, ciudad ubicada en la provincia de Nínive, en el norte de Irak. Sus setenta millas cuadradas están atravesadas por el río Tigris, que sobrepasa la ciudad de noroeste a sureste (Arnold & Fiore, 2019). Dicha batalla inició el 16 de octubre de 2016 y terminó el 20 de julio de 2017, después de que los soldados iraquíes hubieran despejado el último foco de las fuerzas defensoras del Estado Islámico.

Este ejemplo representa sin duda un conflicto urbano *sui generis*, pues a pesar de que las fuerzas iraquíes contaban con la tecnología y los elementos esenciales, les fue muy difícil recuperar la ciudad porque se encontraron con una resistencia yihadista agresiva que utilizaba francotiradores, bombas y vehículos cargados con explosivos. Algunos sitios del sector occidental de Mosul tenían calles estrechas que impedían el paso de los vehículos blindados y obligaban a que las tropas de infantería se internaran y estuvieran desprotegidas. Otra de las dificultades que enfrentaron las fuerzas regulares fue la cantidad de túneles, los cuales retrasaban o impedían su avance.

Estas experiencias también muestran que el desafío en los conflictos urbanos futuros será poner en escena una buena campaña de operaciones psicológicas, entre las cuales suministrar información será esencial para persuadir a los civiles a que abandonen la ciudad. En Mosul, por ejemplo, solo se pudo considerar parcialmente exitosa la intención de difundir mensajes a la población a través de teléfonos celulares, internet y folletos, eliminarlos de forma segura y rápida y,

posteriormente, proveer refugio, alimentos y apoyo médico para evitar más víctimas de la violencia de ambos lados. De hecho, “Mosul demostró que esto puede ser imposible” (Amnistía Internacional, 2017, s.p.).

Como se puede observar, la guerra se libra en áreas urbanas y las personas de esta época están acostumbradas a monitorear este escenario por medio de diferentes medios tecnológicos para estar al tanto de todo. En particular, las ciudades son centros de poder que concentran el control económico, político y social de cualquier civilización actual. Por eso, la necesidad de Rusia de tomarse las principales ciudades de Ucrania en esta guerra, situación que le ha costado trabajo lograr. Adicionalmente, el territorio urbano concentra recursos y elementos que pueden ser utilizados para mantener a la población civil como rehén, lo cual cuestiona el derecho de la guerra y las estrategias de intervención adoptadas por las organizaciones humanitarias.

En el libro *Tridente del poder estratégico: Inteligencia, Operaciones Especiales y poder ciber en el siglo XXI*, González-Martínez y Montero-Moncada (2020) hacen referencia a la aplicabilidad y disposición de las Fuerzas Especiales Urbanas para enfrentar los desafíos de Colombia a futuro. Además, establecen que las Fuerzas Militares del país deben concebir una doctrina que permita preparar estrategias para combatir las nuevas amenazas que han trascendido por causa de la globalización desviada.

Eventos como la toma de la embajada de la República Dominicana en la ciudad de Bogotá, D. C. (el 28 de febrero de 1979), los atentados a las Torres Gemelas en Nueva York (el 11 de septiembre de 2001) y la invasión a Irak (2003) crearon la necesidad de hacer un ajuste a la misionalidad de las Fuerzas Militares y, en particular, de sus FF. EE. En el caso colombiano, según datos de la Comisión Nacional de Memoria Histórica, entre 1965 y 2013 todos los actores armados insurgentes del conflicto interno aplicaron frecuentemente la estrategia de toma de poblados y cabeceras municipales, lo cual llamó la atención regional, nacional y mundial.

En la actualidad, Colombia está enfrentando múltiples desafíos. Por ejemplo, la denominada “primera línea” se ha convertido en un reto en la urbanización del conflicto, dado que utiliza la figura de la protesta pacífica como un escudo perfecto para realizar sus acciones. Al respecto, es importante reconocer que estas protestas han sido el resultado tanto de desequilibrios económicos y sociales graves que el país ha arrastrado desde hace décadas, como de las nuevas tecnologías y sus medios, desde internet hasta las redes sociales.

Este tipo de amenaza contra los intereses de la nación y su seguridad es lo que Guattari (2017) denomina “revolución molecular disipada”. Esa modalidad toma como fuentes históricas las ideas expresadas por Antonio Gramsci, ante la

necesidad de hacer la revolución desde las “supraestructuras” y combinando los medios no violentos con los medios violentos. El fundamento teórico es el presupuesto de que la “revolución molecular” es un sistema universal de lucha social y emancipación (Guattari, 2017).

En virtud de ese fenómeno, la Fuerza Pública, específicamente el Ejército Nacional, dentro de su nueva doctrina (denominada Damasco), señala las capacidades de apoyo a las operaciones urbanas (Ejército Nacional de Colombia, 2017a). Se establece que ellas son parte del concepto operacional del Ejército (Operaciones Terrestres Unificadas [OTU]) y se conducen en Acción Unificada (AU) como parte de la acción decisiva. Particularmente, realizan tareas de Apoyo de la Defensa a la Autoridad Civil (ADAC), las cuales tienen siete propósitos principales: salvar vidas, restaurar los servicios esenciales, mantener o restaurar la ley y el orden, proteger la infraestructura y propiedad (pública y privada), apoyar el mantenimiento o restauración del gobierno local, configurar el ambiente operacional para el éxito interagencial y apoyar la recuperación social del territorio (Ejército Nacional de Colombia, 2017a).

Alcances operacionales y estratégicos de las Fuerzas Especiales en conflictos en megaciudades

La urbanización no controlada podría contribuir al crecimiento de la insurgencia, el terrorismo y otras formas de violencia, cuando las exigencias de las ciudades rebasan las capacidades institucionales. El resultado suele ser que los gobiernos locales son superados por la proliferación de prácticas informales y/o delictivas de la territorialización de grupos criminales. En consecuencia, es fundamental que las Fuerzas Militares y la Policía, dependiendo del país y el contexto, cuenten con unidades que estén capacitadas para actuar como un todo o disgregadas en equipos de combate –conformados por cuatro hombres con especialidades específicas individuales–, que potencien la interdependencia y la libertad de acción al momento del asalto.

Como se mencionó, las Fuerzas Militares de Colombia cuentan con la AFEAU, cuya misión principal es,

conducir operaciones militares especiales de contraterrorismo y otras misiones de Fuerzas Especiales en áreas urbanas y semiurbanas, designadas por el alto mando, contra objetivos militares de alto valor estratégico (OMAVE) y objetivos militares de interés nacional (OMINA) que contribuyen en el cumplimiento de los objetivos del Comando Superior. (Ejército Nacional de Colombia, 2021, p. 32)

Debido a su alto nivel de entrenamiento y al material especial con que cuenta, una unidad de FF. EE. no se limita exclusivamente a la conducción de operaciones de contraterrorismo, sino que, de acuerdo con el análisis del ambiente operacional, puede emplear una o más de sus capacidades distintivas, como el rescate de rehenes y la recuperación de personal, la asistencia a las fuerzas de seguridad, la defensa interna en el extranjero, la evacuación de no combatientes, la acción directa, el reconocimiento especial, entre otras. Al respecto, es importante mencionar la participación destacada que ha tenido esta unidad en la competencia militar denominada “Fuerzas Comando”. Este certamen inició en el año 2004, cuando el Comando Sur de los Estados Unidos, y bajo la responsabilidad del Comando de Operaciones Especiales Sur (SOCSOUTH, por su sigla en inglés), creó y patrocinó competencias para medir las capacidades de cada equipo, fortalecer las relaciones entre los miembros de las Fuerzas Armadas del continente y compartir conocimientos y experiencias adquiridas en la lucha contra el terrorismo.

Por otra parte, la Universidad Conjunta de Operaciones Especiales hace referencia a una serie de tópicos vitales para las Operaciones de FF. EE. Urbanas, como los enfoques del adversario en la guerra política, los puntos ciegos estratégicos en el conflicto moderno y los Derechos Humanos como sistema de armas (Joint Special Operations University, 2021). Esto último se sustenta en la Declaración Universal de los Derechos Humanos de las Naciones Unidas.

Finalmente, es importante resaltar que el Comité Internacional de la Cruz Roja (CICR, 2021), con el fin de minimizar el impacto de la guerra urbana, escribió un manual que sirve como guía de los principales marcos aplicables del Derecho Internacional Humanitario en ambientes operacionales urbanos dirigida a los comandantes en todo nivel.

Estudio de caso: Brasil y Colombia

Los análisis prospectivos sobre el conflicto urbano con motivación intraestatal muestran los desafíos que las FF. EE. van a enfrentar en el futuro. Las implicaciones táctico-operacionales para hacer frente a las amenazas indican alteraciones sustanciales en la gestión de la seguridad. En este contexto, para ilustrar los abordajes teóricos propuestos, se plantea un estudio de caso comparativo entre Brasil y Colombia, con la intención de encontrar convergencias y divergencias en la manera de “operacionalizar” rediseños eficaces para combatir este problema.

Brasil

América Latina sobresale por haber conseguido una mayor velocidad de urbanización en el siglo XX. Brasil es el país más grande de Suramérica y uno de los más poblados –tiene una densidad de 22,5 habitantes por kilómetro cuadrado y su población se triplicó desde el año 1950–, tiene una superficie enorme y cuenta con grandes bosques vírgenes y regiones deshabitadas. Cerca del 86 % de la población vive en ciudades, de la cual cerca de un tercio reside solo en las diez mayores regiones metropolitanas del país (Datosmundial, 2022).

Aunque este estudio de caso se centra en Río de Janeiro, cabe señalar que las otras ciudades más grandes de Brasil son São Paulo, Brasília, Salvador y Fortaleza. Además de sus atributos turísticos, la ciudad de Río de Janeiro es conocida por sus altas tasas de violencia y criminalidad y, junto con São Paulo, se destaca como núcleo de tensión en Brasil. De acuerdo con Lawrence (2019), “las megaciudades se están convirtiendo en epicentros de la actividad humana en todo el planeta y, en consecuencia, generarán la mayor parte de fricciones que requerirán intervención militar” (p. 529).

La violencia de São Paulo tiene que ver más con los mil trescientos atentados cometidos por parte de varios grupos vinculados con la banda de narcotraficantes Primer Comando de la Capital, así como con los amotinamientos en setenta y tres prisiones de la ciudad (Harris et al., 2014, p. 18). Por su parte, la violencia de Río de Janeiro se relaciona con el empleo de más de tres mil agentes de la policía y militares para poner fin a los actos de violencia que se estaban extendiendo por casi toda la ciudad después de haber empezado en una de las seiscientas comunidades (Langewiesche, 2008).

En el escenario contemporáneo, la globalización económica ha dado lugar a un nuevo orden mundial. Queiroz et al. (2022) detallan cuál es su impacto en aquellos Estados con un grado elevado de subdesarrollo, en los cuales emergen actores con motivaciones político-ideológicas sin vínculos con los Estados nacionales y que tratan de imponer su posición mediante el uso de la fuerza, ya que no tienen una representación estatal.

Estas “nuevas amenazas” –insurrecciones, delincuencia organizada, narcotráfico, piratería y terrorismo– le quitan el monopolio de la guerra al Estado, debido a que se presentan como un desafío para las instituciones militares como conjunto. Por ejemplo, en algunos casos, la modalidad de “guerra asimétrica” que proponen ignora el Derecho Internacional de los Conflictos Armados (DICA) y el Derecho del Conflicto Armado (LOAC, por su sigla en inglés), que se rige por los términos de la Convención de Ginebra.

Ciertos elementos de asociación entre criminales y pseudorreligiosos también forman parte de un fenómeno emergente en los conflictos urbanos en Río de Janeiro. De hecho, los delincuentes han encontrado puntos de convergencia con el crecimiento de la matriz evangélica, lo cual ha desencadenado el “narcopentecostalismo” –que trata a creyentes de matrices africanas como enemigos en una especie de yihad del trópico–, movimientos como Bonde de Jesús y territorialización delictiva como Complejo de Israel.

En este punto es importante señalar que el proceso de formación de una unidad de hombres capaces de conducir acciones militares no convencionales (Operaciones Especiales) requiere una combinación de factores que dependen, fundamentalmente, de las políticas nacionales referentes a la seguridad, la iniciativa y la fuerza militar en cuestión (Armada, Ejército o Fuerza Aérea), el aporte económico destinado para ello, la disponibilidad de tiempo (entrenamiento operacional), los recursos existentes (hombres, equipo y armamento), la adecuación y la modernización tecnológica para emplear las habilidades adquiridas, y la experiencia de combate (Denécé, 2009; Lisboa, 2017).

Colombia

Ubicada entre el cruce de Centro y Suramérica, Colombia sirve como un conducto del comercio mundial lícito e ilícito. Para Zambrano y Álvarez (2017), esa característica la convierte en un Estado o región portal, puesto que desempeña un papel geoestratégico sumamente importante al unir diferentes partes del mundo, facilitar el intercambio de personas, bienes e ideas, y cumplir diversas funciones económicas y sociales positivas. Pero en algunos casos, a causa de la globalización desviada, pueden llegar a ser más problemáticos (Zambrano & Álvarez, 2017, p. 290).

Con respecto a la dinámica de expansión demográfica, Colombia enfrenta el flujo migratorio forzado de personas de países vecinos y sus implicaciones sociales, económicas, políticas y a la seguridad nacional. Este país tiene cinco grandes ciudades: Medellín, Cali, Cartagena, Barranquilla y Bogotá, D. C., la capital de Colombia, que está ubicada en el centro del país, genera gran poder geopolítico (Instituto Geográfico Agustín Codazzi, 2022) y tiene una triple condición constitucional: capital de la República, capital del departamento de Cundinamarca y Distrito Capital con régimen especial. Además, según Parag Khanna (2016b), se proyecta como una megaciudad para los próximos años.

En cuanto a la seguridad, ha tenido una carga histórica marcada por diferentes eventos en los últimos treinta años. El incremento de una variedad de grupos

delictivos –auspiciados por organizaciones de dinámicas globalizadas y financiados con recursos del narcotráfico– ha facilitado la comisión de actos terroristas, con un impacto elevado que ha ocasionado el pánico colectivo y social. Este problema no es nuevo, pero deja consecuencias inconmensurables y una huella imborrable en las mentes y corazones de la población.

Lo anterior aumenta el potencial de disturbios, perturbaciones y desorden a gran escala. Al respecto, Kilcullen (2013) pronostica un mundo centrado en megatendencias y resalta los siguientes factores: la urbanización, la litoralización, el conflicto y el rápido crecimiento de la población. Por ese motivo, la fuerza pública tiene múltiples desafíos para proveer una protección adecuada a los activos estratégicos y a la población. Las amenazas actuales tienen acceso a las nuevas tecnologías y emplean esta herramienta de apoyo valiosa para ocultarse, coordinar sus actividades delictivas y realizar acciones armadas con medios irregulares y de sabotaje en ambientes urbanos, que se diferencian de los rurales.

En este sentido, Rojas (2017) señala la necesidad de que el Ejército Nacional de Colombia se enfoque en vencer los desafíos que enfrenta actualmente y en avizorar los del futuro. Esta realidad le exige, en el contexto de sus sistemas de gestión estratégica, considerar continuamente procesos de modernización y adaptación, con el fin de desarrollar capacidades para dar respuestas oportunas, eficaces y sustentables a los requerimientos estratégicos que surgen del estudio del campo de combate.

Conflicto urbano en Río de Janeiro y Bogotá, D. C.

Río de Janeiro y Bogotá, D. C., son símbolos de ciudades desafiadas por la violencia y la criminalidad –como componentes de conflictividad en el ambiente urbano–, aunque conservan sus singularidades –como espejo de la natural e intangible diversidad humana– y tendencias coincidentes. Estas permiten verificar su constitución en megaciudades (Khanna, 2016b) y el conflicto urbano que las agobia (Fidalgo et al., 2010; Mendonça, 2018). En términos estructurales, el corte histórico posterior a la Guerra Fría presenta una mayor intensidad de los conflictos intraestatales, con participación de agentes no estatales, lo que posibilita tener datos tangibles que destacan las complejidades de los rasgos delincuenciales en el orden mundial 2.0, de conformidad con lo propuesto por Queiroz et al. (2022).

En el ejercicio comparativo entre Río de Janeiro y Bogotá, D. C., cada una de estas ciudades representa una cultura y provee un imaginario divergente con aspectos positivos (por ejemplo, el turismo) y negativos (como la sensación de inseguridad).

El ambiente de inseguridad involucra a diferentes organizaciones criminales y milicias. Desde finales del siglo XX, los conflictos en el mundo han mutado y han adquirido una índole más intraestatal que interestatal, por causa de la aparición de actores armados violentos no estatales. Al respecto, Muggah (2017) sostiene que este nuevo tipo de conflicto se da por la confluencia entre el crimen organizado y la guerra abierta, lo que ha retado las reglas tradicionales de los enfrentamientos urbanos.

El surgimiento de conflictos urbanos exige la evolución constante de capacidades, armas y doctrina de mando, control y comunicaciones. A su vez, esto tiene una indudable influencia en la vida cotidiana de millones de ciudadanos que viven en los vecindarios de los barrios marginales de Río de Janeiro y São Paulo, en donde el control estatal es limitado o inexistente.

Grupos criminales como el Comando Rojo y el Tercer Comando (Bartolomé, 2019) han podido prosperar en Brasil debido a las limitaciones de la actividad policial y la falta de eficacia en la gestión de la seguridad. En este escenario, los delincuentes urbanos se han valido de la incapacidad del Estado para encontrar respuestas a las disparidades socioeconómicas. Los traficantes de armas y drogas, las milicias, las pandillas y hasta los pseudorreligiosos desestabilizan los mecanismos estatales y aterrorizan a los residentes de las comunidades, manteniéndolos como rehenes mientras conservan bajo control al gobierno y a su aparato institucional.

Sin embargo, frente a estos escenarios el presidente de Brasil puede decretar operaciones para garantizar la ley y el orden (GLO), de acuerdo con las leyes complementarias 97/1999 y 117/2004 (Presidência da República do Brasil, 1999, 2004), según las cuales es posible convocar a las Fuerzas Armadas para que ayuden a tomar el control. Precisamente, una diferencia notable con Colombia es el papel expansivo que pueden asumir las Fuerzas Armadas brasileñas.

En referencia a la ciudad de Bogotá, D. C., su análisis muestra parámetros singulares. Teniendo en cuenta la información de contexto de sus antecedentes, la dinámica actual de su conflicto presenta mayor complejidad e involucra múltiples combinaciones de actores, en comparación con varios sucesos históricos que marcaron la violencia del siglo XX. Sin lugar a duda, el hecho que marcó el hito del conflicto colombiano fue el asesinato del candidato presidencial Jorge Eliécer Gaitán, sucedido en la capital el 9 de abril de 1948, lo cual produjo una serie de disturbios y manifestaciones del pueblo en lo que se conoce como “El Bogotazo”.

Hasta la década de los años ochenta, la violencia en Bogotá se debía al conflicto armado, no había acciones del narcotráfico o del crimen organizado. No obstante, también es fundamental tener en cuenta los hechos mencionados sobre las tomas de la embajada de la República Dominicana y del Palacio de Justicia por parte del M-19.

Algunas de las modalidades que han empleado los actores del conflicto a partir de los años ochenta se configuraron como un rasgo propio en Bogotá, D. C., para sostener, imponer o disputar su control territorial: el homicidio, la trata de personas, la extorsión, el microtráfico, etc. Una parte importante de los fenómenos experimentados durante estos últimos años se debe al negocio lucrativo del microtráfico, la disputa por el control de las localidades y la presencia de varios grupos criminales articulados y coordinados por mandos externos. Una de las zonas de mayor peligrosidad en Bogotá es la que se conoce como “Bronx”, ya que allí convergen varios delitos y se ve una alta tasa de necesidades básicas insatisfechas (NBI) (Avendaño et al., 2019; Escobar, 2020).

Al ser una ciudad epicentro, es receptora de un gran número de desplazados que huyen del conflicto interno del país, de manera que se multiplican los factores de criminalidad, se desata una ola de violencia y pugna por el control del microtráfico, y se producen daños colaterales en el desarrollo y la convivencia ciudadana.

Como se aprecia, tanto Río de Janeiro como Bogotá, D. C., han sido foco de bandas delincuenciales que se han apropiado de ciertas zonas, ante las dificultades de un Estado efectivo, en las cuales han creado un ambiente de temor y miedo en la comunidad que les permite mantener un control absoluto de lo que sucede en sus territorios. Por lo general, estas bandas usan el microtráfico como medio para ampliar sus negocios y conseguir recursos para financiar mafias establecidas en el tiempo, lo cual crea guerras internas entre minicarteles y lleva a un recrudecimiento de la guerra.

De este modo, se encuentra que la delincuencia se ubica más en las zonas de concentración demográfica interrelacionadas con el conflicto y sostenidas por gobiernos débiles y por la inestabilidad política. Esto permite verificar de manera empírica la hipótesis relacional directa de que cuanto mayor sea el grado de fragilidad del Estado, mayor es la probabilidad de que se produzcan acciones conflictivas ancladas en el uso de la violencia y la fuerza para provocar un estado de terror en pos de los objetivos políticos y/o ideológicos de los grupos delictivos (Queiroz et al., 2022).

Conclusiones

Esta investigación tuvo como objetivo analizar los desafíos de las FF. EE. en futuras megaciudades, los cuales se verificaron empíricamente, por comparación, en las ciudades de Río de Janeiro y Bogotá, D. C. Además, se propuso hacer un análisis prospectivo referente a la evolución constante de los conflictos en megaciudades como escenario de conflicto y al empleo de la fuerza pública por intermedio de unidades de FF. EE.

Los estudios sobre conflictos pocas veces mencionan ciudades como escenario de confrontación y se suele desconocer si estas son afectadas directa o indirectamente por las consecuencias de las hostilidades. De hecho, en cada uno de los períodos de la evolución humana ha habido ciudades que han sido destruidas con técnicas específicas de conflicto urbano, como el uso del asedio en la Antigüedad o la Edad Media.

En lo concerniente a la seguridad y la defensa de los Estados, el 11 de septiembre de 2001 marcó un referente de las capacidades y alcances de las amenazas, cuando dos aviones impactaron y destruyeron los símbolos del poder económico y militar de los Estados Unidos. Este hecho demuestra la susceptibilidad de las ciudades como blancos de diferentes tipos de ataques terroristas.

El fenómeno de las amenazas en las áreas urbanas, visto desde varias aristas, se sintetiza en un concepto conjunto de la criminalidad: la convergencia (Luis Alexander Montero Moncada, entrevista realizada por M. A. Cabra en 2022). En él coinciden varios factores, como los crímenes organizados transnacionales y los elementos delincuenciales, los cuales funcionan como redes entrelazadas que buscan debilitar la democracia y la gobernanza, con la intención de crear las condiciones para infiltrar o dominar las ciudades.

Antecedentes como los mencionados en este capítulo respaldan la tendencia de que las operaciones urbanas dominarán los conflictos del siglo XXI. El crecimiento constante de la urbanización, los cambios de una sociedad diversa y la persistencia de las amenazas y los peligros contribuyen a que el conflicto se agudice, ya que existen muchos incentivos políticos y económicos para que los adversarios de los Estados decidan escoger este escenario como su centro de gravedad.

En este contexto, es importante aplicar y transversalizar el derecho operacional en el Proceso Militar para la Toma de Decisiones (PMTD). Entre otros desafíos, está la decisión de determinar cuál será el parámetro de medición para usar la fuerza en cada situación; igualmente, es relevante ajustar y considerar el empleo de los

principios que orientan las actuaciones durante las hostilidades, entre los cuales se encuentran la necesidad militar, la distinción, la proporcionalidad, la limitación, la no reciprocidad, la humanidad y la precaución en el ataque (Ejército Nacional de Colombia, 2017b).

En cuanto a las actuaciones de las Fuerzas Militares, los resultados de la investigación evidencian la necesidad de tener consideraciones adicionales. Por ejemplo, el uso de las armas durante el desarrollo de las operaciones militares debe estar sujeto a un marco jurídico y condicionado a un amplio espectro de reglas, principios y normas de origen convencional. Asimismo, debe fundamentar su legitimidad en la aplicación de los principios rectores del Derecho Internacional Humanitario (DIH) y el Derecho Internacional de los Derechos Humanos (DIDH), los cuales son marcos jurídicos que se complementan, coexisten y convergen en los conflictos armados no internacionales (CANI), de conformidad con los Convenios de Ginebra (Ejército Nacional de Colombia, 2017b).

En este sentido, las FF.EE. se deben mantener en un ejercicio constante de analizar y evaluar las lecciones aprendidas, entre las cuales se incluyen las que han tenido las Fuerzas Armadas de diferentes países. Esto les permitirá consultar, en el campo de la defensa y de la seguridad, ciertas reacciones ante situaciones de gestión de crisis contra una naturaleza cambiante y adaptativa de las actividades delictivas.

La investigación demuestra que las alianzas con los países que tienen el mismo común denominador como amenaza permiten afianzar la consulta y potenciar la interoperabilidad en un trabajo sinérgico constante. Estos contextos son apropiados para verificar la conveniencia de conducir operaciones multinacionales de gestión de crisis y generar los mecanismos adecuados de intercambio de procedimientos e inteligencia para la interacción militar, con agencias gubernamentales y no gubernamentales, fuerzas multinacionales y otros socios interinstitucionales.

El aporte principal de este estudio es que presenta un rol clave para las FF. EE. Se subraya la necesidad de constituir mecanismos versátiles a fin de crear un planeamiento detallado, conveniente y efectivo, con una distribución correcta de los medios que permita identificar el centro de gravedad del enemigo (con su fuente de poderío y de resistencia moral) y limitar su libertad de acción, con el fin de dirigir el esfuerzo militar de modo eficaz.

En este sentido, es esencial resaltar que las Fuerzas Militares de Colombia y de otros países se han ido adaptando a un escenario cambiante, de manera que las unidades militares de FF. EE. estarán siempre entrenadas, capacitadas,

certificadas y especializadas en capacidades críticas de acuerdo con las necesidades sociopolíticas.

Finalmente, si bien el estudio de caso comparativo entre Brasil y Colombia presenta puntos similares y contrastantes, en un escenario prospectivo reitera que la delincuencia tiende a asumir diversas formas y deja entrever que las FF. EE. siempre tendrán que hacer frente a desafíos adicionales que no fueron investigados en este trabajo. La mejor manera de aproximarse a la solución de los conflictos o las crisis que se presenten en los ambientes urbanos es adquirir la conciencia de que es necesario mantener un carácter cambiante que potencie la efectividad en la protección. Prevenir, adaptarse y planear con antelación es la mejor forma de cumplir la misión con eficacia en un escenario de conflicto en megaciudades y garantizar la estabilidad y la seguridad de la población.

Referencias

- Álvarez, C. E., Barón, P., & Monroy, V. (2018). Poder astuto: Estrategia del empleo del poder en el siglo XXI. En C. Álvarez Calderón & A. Fernández Osorio (Eds.), *Hacia una gran estrategia en Colombia: Construcción de política pública en seguridad y defensa* [vol. 1: *La "Gran Estrategia": Instrumento para una política integral en seguridad y defensa*] (pp. 171-168). Sello Editorial ESMIC. <https://doi.org/10.21830/9789585692862>
- Alves, L. A. (2018). *A interação civil-militar na situação de não guerra: Uma análise das lições da MINUSTAH* [Presentación de artículo]. 10 Encontro da Associação Nacional de Estudos de Defesa, São Paulo, Brasil. <https://tinyurl.com/4jjeas3w3>
- Amnistía Internacional. (2017, 11 de julio). A cualquier precio: La catástrofe civil del oeste de Mosul, Irak. <https://tinyurl.com/2ey8432h>
- Arnold, T. D., & Fiore, N. (2019). Five operational lessons from the battle for Mosul. *Military Review*, (enero-febrero), 58-71. <https://tinyurl.com/4ndbyzj3>
- Avendaño Arias, J. A., Forero Flórez, J. A., Oviedo Yate, B. S., & Trujillo Vanegas, M. Y. (2019). Entre el Cartucho y el Bronx en Bogotá: ¿Territorios del miedo o expresiones de injusticia socioespacial? *Cuadernos de Geografía: Revista Colombiana de Geografía*, 28(2), 442-459. <https://doi.org/10.15446/rcdg.v28n2.73531>
- Bartolomé, M. C. (2019). Terrorismo y crimen organizado en Sudamérica [Documento de Investigación, n.º 2]. Instituto Español de Estudios Estratégicos. <https://tinyurl.com/2p99hcs3>
- Cazumba, R. A. (2021). O conceito de centro de gravidade: Seu emprego como ferramenta de planejamento nos EUA e no Brasil. *Hoplos*, 5(9), 9-31. <https://tinyurl.com/yjepvfta>
- Comando General de las Fuerzas Militares [CGFM]. (2016). Disposición N.º 004 de 2016, "por la cual se reestructura el Ejército Nacional, se aprueban sus Tablas de Organización y Equipo TOE y se dictan otras disposiciones". <https://tinyurl.com/dxxv6da3>
- Comisión Económica para América Latina y el Caribe [CEPAL]. (1989). *La crisis urbana en América Latina y el Caribe: Reflexiones sobre alternativas de solución*. Organización de las Naciones Unidas. <https://tinyurl.com/mvn3p82b>
- Comisión Económica para América Latina y el Caribe [CEPAL]. (2015). Objetivos de Desarrollo Sostenible (ODS). <https://tinyurl.com/2pcbr9d3>
- Comité Internacional de la Cruz Roja [CICR]. (2021, 5 de noviembre). Reducción del daño civil en la guerra urbana: Manual del comandante. <https://tinyurl.com/nemctjyh>
- Datosmundial. (2022). Crecimiento demográfico en Brasil. <https://tinyurl.com/mva4tjzx>
- Denécé, E. A. (2009). *A história secreta das Forças Especiais: De 1939 a nossos dias*. Larousse do Brasil.
- Ejército Nacional de Colombia. (2017a). *Manual Fundamental del Ejército MFE 1.0 El Ejército* [Público]. Imprenta Militar del Ejército. <https://tinyurl.com/45sujuw5>
- Ejército Nacional de Colombia. (2017b). *Manual Fundamental del Ejército MFE 6-27 Derecho Operacional Terrestre* [Público]. Imprenta Militar del Ejército <https://tinyurl.com/2s3627j3>

- Ejército Nacional de Colombia. (2019). Disposición N.º 000002 de 2019, “por medio de la cual se reglamentan las reglas de enfrentamiento relativas al uso de la fuerza en las operaciones militares que desarrolla el Ejército Nacional en el marco de los Derechos Humanos y del Derecho Internacional Humanitario”. Departamento Jurídico Integral. <https://tinyurl.com/458ry7dc>
- Ejército Nacional de Colombia. (2021, 13 de septiembre). Agrupación de Fuerzas Especiales Antiterroristas. Ejército Nacional. <https://tinyurl.com/3d7e47b8>
- Escobar Correa, C. (2022). Should a human rights-based approach to the homeless be used in the neoliberal city? Case study in Bogotá, Colombia. *Latin American Law Review*, 1(8), 111-124. <https://doi.org/10.29263/lar08.2022.07>
- Escuela Superior de Guerra “General Rafael Reyes Prieto” [ESDEG]. (2021). *Revista Fuerzas Armadas*, 41(257) [Protesta social: una visión desde la academia]. <https://tinyurl.com/mr4d2uzz>
- Espinosa, A. (2017, 14 de junio). La mitad de los civiles muertos en guerras fallecieron en Siria, Irak y Yemen. <https://tinyurl.com/4thuudt7>
- Fidalgo, A. S., Suárez, C. J., Vallejo, E., & Brasil, A. (2010). Faces da ilegalidade em Bogotá. *Tempo Social*. 22(2), 123-142. <https://doi.org/10.1590/S0103-20702010000200007>
- Freedman, L. (2019). *La guerra futura: Un estudio sobre el pasado y el presente*. Planeta.
- González-Martínez, M. A., & Montero-Moncada, L. A. (Eds.). (2020). *Tridente del poder estratégico: Inteligencia, Operaciones Especiales y poder ciber en el siglo XXI*. Sello Editorial ESDEG. <https://doi.org/10.25062/9789584288943>
- Guattari, F. (2017). *Revolución molecular*. Errata Naturae.
- Harris, L. C., Dixon, R., Melin, N., Hendrex, D., Russo, R., & Bailey, M. (2014). *Megacities and the United States Army: Preparing for a complex and uncertain future*. Chief of Staff of the Army; Strategic Studies Group. <https://tinyurl.com/2hwmuduv>
- Iberdrola. (2020). Megaciudades, un reto de futuro. <https://tinyurl.com/4cux4nuf>
- Instituto Geográfico Agustín Codazzi [IGAC]. (2022). Colombia en mapas. <https://tinyurl.com/y4cexwer>
- Izquierdo, J. C. (2018). Cisnes, elefantes, medusas y rinocerontes: Las relaciones internacionales y sus animales. *Comillas Journal of International Relations*, (12), 1-8. <https://doi.org/10.14422/cir.i12.y2018.001>
- Joint Special Operations University. (2021). *Special Operations Research Topics 2022*. The JSOU Press. <https://tinyurl.com/yjs9tsk3>
- Khanna, P. (2016a). *Conectografía, mapear el futuro de la civilización mundial*. Paidós.
- Khanna, P. (2016b). How megacities are changing the map of the world [TED Talks]. YouTube. <https://www.youtube.com/watch?v=U7y4GlmwPLQ>
- Kilcullen, D. (2013). *Out of the mountains: The coming age of the urban guerrilla*. Oxford University Press.

- King, A. D. (2008). Architecture, globalization and identity. En P. Herrle & E. Wegerhoff (Eds.), *Architecture and identity* (pp. 221-232). LIT.
- Langewiesche, W. (2008, 20 de marzo). City of fear. *Vanity Fair*. <https://tinyurl.com/4rcxf3yk>
- Lawrence, F. (2019). *La guerra futura: Un estudio sobre el pasado y el presente*. Crítica.
- Lehmann, A. P. (2015, 15 de enero). ¿Ciudades en crecimiento, peligro en crecimiento? <https://tinyurl.com/j65zr6xw>
- Lisboa, R. A. P. (2017). Avançando pelo labirinto: Procedimentos de progressão em ambiente urbano por FOPEsp [e-mail]. *Revista Segurança e Defesa*, (127). s. p.
- Mendonça, M. J. (2018). A cidade como espaço de batalha: De Gaza ao Rio de Janeiro, *GEOUSP. Espaço e Tempo*, 21(3), 685-702. <https://doi.org/10.11606/issn.2179-0892.geousp.2017.105565>
- Morán, C. (2021, 23 de abril). Las seis ciudades más violentas del mundo están en México. *El País*. <https://tinyurl.com/2n46ayd2>
- Muggah, R. (2017). El auge de la seguridad ciudadana en América Latina y el Caribe. *International Development Policy*, (9). s. p. <https://doi.org/10.4000/poldev.2512>
- Organización de las Naciones Unidas [ONU]. (2015). La Asamblea General adopta la Agenda 2030 para el Desarrollo Sostenible. <https://tinyurl.com/2p8sfnpk>
- Organización de las Naciones Unidas [ONU]. (2018a). Porcentaje urbana e de aglomeración urbana en 2030 [Base de datos]. <https://tinyurl.com/ybesp72r>
- Organización de las Naciones Unidas [ONU]. (2018b). Transformar nuestro mundo: la Agenda 2030 para el Desarrollo Sostenible. <https://tinyurl.com/yc4bu4z9>
- Organización de las Naciones Unidas [ONU]. (2018c). Tasa de crecimiento de aglomeración urbana (2018-2030) [Base de datos]. <https://tinyurl.com/ybesp72r>
- Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura [Unesco]. (2017). *Cultura: Futuro urbano, informe mundial sobre la cultura para el desarrollo urbano sostenible*. UNESCO. <https://tinyurl.com/4eds2sn7>
- Presidência da República do Brasil. (1999). Lei Complementar N.º 97 de 9 de junho de 1999. Dispõe sobre as normas gerais para a organização, o preparo e o emprego das Forças Armadas. <https://tinyurl.com/mr3445dn>
- Presidência da República do Brasil. (2004). Lei Complementar N.º 117 de 2 de setembro de 2004. Altera a Lei Complementar no 97, de 9 de junho de 1999, que dispõe sobre as normas gerais para a organização, o preparo e o emprego das Forças Armadas, para estabelecer novas atribuições subsidiárias. <https://tinyurl.com/ycys4w6f>
- Queiroz, F. A., Cunha, G. L., & Correa, A. J. (2022). Terrorismo em Estados Frágeis na Ordem Mundial 2.0: Um estudo exploratório da África Subsaariana. *Omnidef Analysis*, 5(2), 3-14. <https://tinyurl.com/yftnd66a>
- Rojas Guevara, P. J. (2017). Doctrina Damasco: Eje articulador de la segunda gran reforma del Ejército Nacional de Colombia. *Revista Científica General José María Córdova*, 15(19), 95-119. <https://doi.org/10.21830/19006586.78>

- Santos, M. (2004). *O espaço dividido*. EDUSP.
- Spencer, J. (2022). Cuenta de Twitter analista militar guerra urbana. <https://bit.ly/3Df8cow>
- Urban Agenda Platform. (2002). The New Urban Agenda. <https://tinyurl.com/3rrhp7zr>
- Valdés-Ramírez, J. C., & Rodríguez-Gómez, A. (Eds.). (2020). *Memorias imborrables: Guardías de honor*. Sello Editorial ESDEG. <https://doi.org/10.25062/9789584289001>
- Wigmore, I. (2017). VUCA (volatilidad, incertidumbre, complejidad y ambigüedad). <https://tinyurl.com/nhemcc8j>
- Wucker, M. (2016). *The Gray Rhino: How to recognize and act on the obvious dangers we ignore*. St. Martin's Press.
- Zambrano Gómez, J. A., & Álvarez Calderón, C. (2017). *Globalización desviada: Plataforma de convergencia criminal* [Tesis de Maestría, Escuela Superior de Guerra "General Rafael Reyes Prieto"]. ESDEG.

Capítulo 4

Amenazas cibernéticas contemporáneas: retos y desafíos para las operaciones especiales en Colombia^{*}

DOI: <https://doi.org/10.25062/9786287602809.04>

José Nicolás Rodríguez Rodríguez

Escuela Superior de Guerra "General Rafael Reyes Prieto"

Oscar Garzón

Comando Conjunto de Operaciones Especiales

Resumen: Este capítulo hace un estudio comprensivo sobre los retos y desafíos que tienen las unidades de Fuerzas Especiales de Colombia en escenarios de amenazas cibernéticas, caracterizados por lo regular e irregular, el empleo de medios técnicos y tecnológicos elaborados, operaciones de información, ciberataques, altas capacidades de manipulación de información y otros. Para esto, se identifican los efectos de las amenazas cibernéticas contemporáneas a partir de sus elementos constitutivos y se analiza la naturaleza de estas nuevas confrontaciones para explorar las fortalezas y debilidades de las Fuerzas Especiales. De esta manera, se propone la inmersión total de estas unidades en la era digital, preparándolas para el combate en el ciberespacio y motivándolas para su adaptación en áreas críticamente sensibles, como es el quinto elemento de la guerra.

Palabras clave: amenazas; capacidad; cibernética; guerra.

^{*} Este capítulo es resultado de investigación adscrito al proyecto "Naturaleza de la guerra contemporánea. Retos y oportunidades de las Fuerzas Especiales y la Inteligencia", adscrito al Departamento Ejército de la Escuela Superior de Guerra, inscrito en la línea de investigación "Naturaleza de la guerra, terrorismo, nuevas amenazas", que forma parte del grupo de investigación Centro de Gravedad, categorizado en A por Monciencias, con código COL0104976. Los puntos de vista pertenecen a los autores y no reflejan necesariamente los de las instituciones participantes.

José Nicolás Rodríguez Rodríguez

Teniente Coronel del Ejército Nacional del Arma de Fuerzas Especiales de Colombia. Magíster (cum laude) en Ciberdefensa y Ciberseguridad, Escuela Superior de Guerra "General Rafael Reyes Prieto", Colombia. Especialista en conducción de unidades militares y especialista en Administración de Recursos para la Defensa Nacional, Escuela de Armas y Servicios del Ejército Nacional. Profesional en Ciencias Militares, Escuela Militar de Cadetes "General José María Córdova", Colombia. Administrador de empresas, Universidad Politécnica Grancolombiano. Contacto: jose.rodriguezrod1@buzonejercito.mil.co

Oscar Garzón

Coronel del Ejército Nacional del Arma de Fuerzas Especiales de Colombia. Magíster en Estrategia y Geopolítica y diplomado en Estado Mayor, Escuela Superior de Guerra "General Rafael Reyes Prieto", Colombia. Magíster en Estudios de Guerra, King's College London. Profesional en Ciencias Militares, Escuela Militar de Cadetes "General José María Córdova", Colombia.

<https://orcid.org/0009-0001-5826-9008> - Contacto: oscar.garzon@buzonejercito.mil.co

Citación APA: Rodríguez Rodríguez, J. N., & Garzón, O. (2024). Amenazas cibernéticas contemporáneas: Retos y desafíos para las operaciones especiales en Colombia. En L. A. Montero Moncada & O. A. Garzón Gómez (Eds.), *Comandos: Retos de las Fuerzas Especiales e Inteligencia en la guerra contemporánea* (pp. 93-114). Sello Editorial ESDEG. <https://doi.org/10.25062/9786287602809.04>

COMANDOS: RETOS DE LAS FUERZAS ESPECIALES E INTELIGENCIA EN LA GUERRA CONTEMPORÁNEA

ISBN impreso: 978-628-7602-79-3

ISBN digital: 978-628-7602-80-9

DOI: <https://doi.org/10.25062/9786287602809>

Colección Seguridad y Defensa

Sello Editorial ESDEG

Escuela Superior de Guerra "General Rafael Reyes Prieto"

Bogotá D.C., Colombia

2024



Introducción

El bagaje de información sobre el desarrollo de operaciones en el ciberespacio ha escalado a un nivel superior, lo cual permite a las entidades de seguridad y defensa desarrollar habilidades o especialidades distintivas en cada institución o Fuerza. Frente a un aumento exponencial del concepto e importancia de la ciberseguridad en el mundo,

[...] los actores gubernamentales y no gubernamentales han desarrollado capacidades cibernéticas, tanto ofensivas como defensivas, que han desencadenado una reexaminación de las nociones tradicionales del poder global, la influencia e incluso la guerra. (Junta Interamericana de Defensa, 2020, p. 5)

Diversas estrategias institucionales se han implementado para hacer frente a los diferentes riesgos y amenazas que se han identificado en el ciberespacio, lo cual permite explorar nuevas iniciativas en el desarrollo de operaciones militares y, principalmente, en su inclusión directa en áreas como las Fuerzas Especiales (FF. EE.).

El empleo de las FF. EE. en cualquier nación tiene el propósito primordial de defender la soberanía nacional, la independencia, la integridad territorial y el orden constitucional, tanto de amenazas internas como externas. El cumplimiento de este objetivo siempre está bajo el poder del control civil, ejercido por mandato constitucional por el presidente de la República como comandante supremo de las Fuerzas Militares (Ejército Nacional de Colombia, 2018).

Como tesis se plantea que existen retos y desafíos para las Operaciones Especiales (OO. EE.) en Colombia. Teniendo en cuenta las implicaciones relacionadas con el uso de ataques cibernéticos, su empleo por parte de las unidades

de FF. EE. resulta de suma importancia, principalmente al enfrentar fuerzas antagonistas que ponen en riesgo la seguridad y la defensa nacionales. Por lo tanto, el revestimiento doctrinario y de empleabilidad de estas capacidades ofensivas y defensivas puede representar una ventaja de carácter estratégico en la realización de las operaciones militares y, principalmente, en las OO. EE.

Sobre todo en un contexto en el que "las amenazas cibernéticas en los conflictos contemporáneos afectan a la seguridad del hemisferio occidental, siendo cada vez más frecuentes, complejas, destructivas y coercitivas" (Junta Interamericana de Defensa, 2020, p. 5). Esta situación obliga a los actores gubernamentales y principalmente a las organizaciones de seguridad y defensa, como las FF. EE. de Colombia, a plantearse la necesidad de introducir en su doctrina los desafíos que trae consigo el quinto dominio de la guerra. Para hacerlo, se deben analizar los acontecimientos históricos de carácter nacional e internacional, entender el sistema cibernético y sus componentes (Patiño, 2019), determinar los retos y los desafíos que representa el auge de las amenazas cibernéticas en las OO. EE. en Colombia, y analizar algunos temas de referencia con la finalidad de potenciar esta capacidad.

En este orden de ideas, cabe destacar el documento *Alfabetización y seguridad digital: la importancia de mantenerse seguro e informado*, desarrollado por la Organización de los Estados Americanos (OEA, 2019) y Twitter (ahora llamada X), que pretende informar y concientizar a las personas sobre el manejo, el consumo y la distribución de la información en línea, con un enfoque mayor en las redes sociales y toda la estructura a nivel social, los cuales relacionan a los individuos en un dominio digital. Además, tiene el propósito de contribuir a que todas las personas, autoridades gubernamentales y organizaciones logren una mejor comprensión sobre la importancia de la alfabetización y la seguridad cibernética. De esta manera, proyecta de qué forma deben emplearlas las unidades de FF. EE. para que saquen el mayor provecho del mal uso que el enemigo hace de estas.

El incremento de las actividades digitales ha evidenciado vulnerabilidades pre-existentes del espacio digital. El crecimiento en el número de ataques cibernéticos y la digitalización de innumerables procesos cotidianos reafirman la necesidad de aumentar la alfabetización y la concientización de buenas prácticas de ciberseguridad (Nivea & Gazapo, 2016). Esta edición de la guía brinda una visión renovada sobre herramientas, buenas prácticas para consumir información y contenido de manera segura y responsable.

Las plataformas tecnológicas y las redes sociales han creado nuevas modalidades de comunicación, las cuales han ampliado las posibilidades de participación política al permitir que el entorno digital esté involucrado en los procesos democráticos. La alfabetización digital es esencial para el fortalecimiento de la democracia, dado que es un instrumento que contribuye a una participación masiva que facilita una participación ciudadana activa y responsable. De igual manera, la alfabetización contrarresta fenómenos como la desinformación, la injerencia de actores externos en política interna, entre otros elementos, que directa o indirectamente impactan e influyen en los procesos democráticos.

A través de sus diferentes secciones, la guía recopila información sobre la ciberseguridad y el autocuidado digital, la cual ha sido actualizada para presentar las nuevas amenazas y herramientas surgidas a raíz de los cambios en el entorno y el aumento del teletrabajo. Asimismo, incluye recomendaciones específicas en relación con el consumo de información de Twitter y la actualización de sus reglas de uso, así como herramientas fundamentales para la experiencia de las personas en la plataforma.

Todo esto nos lleva a reflexionar que el uso intensivo de las tecnologías digitales en el mundo permanecerá en la vida cotidiana, por lo que la ciberseguridad y la alfabetización, aplicadas por cada individuo, son sumamente importantes para garantizar que puedan capitalizar el beneficio de la conectividad y la disponibilidad de la información de modo seguro. De esta manera será factible brindar un entorno de mayores posibilidades de desarrollo, así como de bienestar social y fortalecimiento de la democracia en una nación.

Así las cosas, la pregunta de investigación resultante es: ¿Cuál debería ser el mecanismo con el cual las OO. EE. de Colombia pueden enfrentar los retos que presentan las amenazas cibernéticas actuales? Es importante recabar que las operaciones de las FF. EE. son de carácter estratégico para la nación, de forma que dicha misionalidad, aplicada a un escenario de guerra híbrida dentro de un ambiente cibernético (Colom, 2012), permite poner en práctica sus capacidades de guerra no convencional.

Específicamente, esta última se enfoca en las vulnerabilidades de una sociedad civil y militar que tradicionalmente no se contemplan a simple vista, lo cual les permite mantener por debajo de ciertos umbrales de detección y respuesta el diseño específico para influir en todo tipo de ambiente operacional y ejecutar acciones letales y no letales, tanto en el país como en el extranjero (Mitaritonna, 2019). Estas características proporcionan un amplio contexto estratégico para emplear

las capacidades de las FF. EE. en relación con otros instrumentos del poder nacional, como las amenazas cibernéticas a la seguridad y defensa nacionales (Realpe & Cano, 2020).

En cuanto a la situación específica de Colombia, se debe señalar que las amenazas cibernéticas impuestas por las tecnologías disruptivas a las Fuerzas de la ley del Estado sugieren una peligrosa tendencia a comprometer la seguridad y la defensa nacionales. Para mitigar estos riesgos, se requiere una estrategia integral que contrarreste, si es necesario, la resistencia a los ataques disruptivos y destructivos, la cual debe estar enmarcada en una transformación digital (Plan Nacional de Protección y Defensa para la Infraestructura Crítica Cibernética de Colombia, 2017).

En efecto, este documento presenta un análisis general de la situación actual en el campo de la ciberdefensa en Colombia. Con este propósito, identifica y toma como referencia las ciberamenazas latentes y emergentes mediante el instrumento denominado Ventana AREM (acrónimo de amenazas y riesgos emergentes). Según Realpe y Cano (2020), esta herramienta de análisis aborda siete tecnologías disruptivas analizadas a corto plazo, con el fin de proponer una estrategia militar de ciberdefensa que les permita a las organizaciones –como las FF. EE.– una inmersión tecnológica para responder a las ciberamenazas con una visión estratégica, integral, sistémica y prospectiva.

En adición a lo anterior, aparece en escena como protagonista una organización con unidades altamente entrenadas, capacitadas, móviles, flexibles y adaptativas, capaces de operar en un ambiente volátil, incierto, complejo y ambiguo (VICA) de manera autónoma, durante largos períodos y con un valor estratégico relevante para una nación, con la necesidad apremiante de mejorar su dinámica operacional e implementar nuevas capacidades conscientes en el quinto dominio de la guerra.

Amenazas a la seguridad y defensa de Colombia con capacidades cibernéticas

Para identificar las fortalezas y debilidades de las operaciones de seguridad y defensa en el quinto dominio de la guerra resulta necesario develar la naturaleza de las nuevas confrontaciones que surgen en la era digital. El ciberespacio no es en sí un entorno seguro, ni protegido, de modo que es vulnerable a las amenazas o

ataques cibernéticos latentes o emergentes. Esto puede resultar en pérdidas significativas para los sectores económicos, políticos y sociales, así como constituir un serio riesgo para la defensa o los intereses nacionales. Por lo tanto, el desarrollo de capacidades en el ciberespacio constituye una prioridad para la seguridad y la defensa de Colombia, que cada vez es más dependiente de la tecnología, de modo que el despliegue de operaciones militares en el ciberespacio es una necesidad para el avance de los modelos de defensa actuales (Sánchez & Rodríguez, 2010).

Día tras día el panorama parece producir una nueva clase de amenazas, cada una más evolucionada tecnológicamente que la anterior, pues aprovecha la detonación masiva de la tecnología. En este escenario, entre los riesgos que pueden vulnerar a una nación se encuentran: la proliferación de información y la facilidad que tienen las personas para comunicarse desde cualquier medio; la conectividad de red a nivel global; el trabajo remoto en la modalidad informal; el empleo negativo del ciberespacio para desarrollar actividades ilegales y la degradación en el manejo de las redes sociales.

En respuesta a esta situación, se ha suscitado un interés cada vez mayor de la comunidad de especialistas en garantizar la seguridad y la defensa de las naciones, descifrar el papel de las unidades de FF. EE. y enfrentar las amenazas emergentes propias de las actividades que realiza el sistema internacional contemporáneo. Por esta razón, desde el punto de vista operacional, la acción de los ejércitos modernos incluye la ciberseguridad, la ciberdefensa, las operaciones de información, la guerra electrónica, la ciberguerra, la guerra híbrida y demás conceptos que abarcan un amplio espectro de riesgos que no habían sido contemplados en las funciones tradicionales y capacidades de las Fuerzas Militares (Miguel-Gil, 2019).

Para comprender los esfuerzos que hacen los Estados para garantizar su seguridad y defensa en los escenarios digitales, es clave conocer la teoría del realismo y, particularmente, la teoría de Hans Morgenthau sobre el carácter estatocéntrico. De acuerdo con Barbe (1987), según este modelo cada Estado es un actor racional que actúa siempre según sus intereses y con el objetivo principal de garantizar su propia seguridad. Con este propósito, define e implementa ciertos parámetros que conciernen a la defensa de su soberanía, como objetivo exclusivo de las relaciones internacionales, y a la protección de sus intereses de defensa mediante el poder militar o el *soft power*.

En este sentido, definir una propuesta de estrategia militar de ciberdefensa constituye una respuesta efectiva a los riesgos y las amenazas cambiantes a los que se enfrenta la seguridad y la defensa de un país de cara a las tecnologías

disruptivas en un conflicto contemporáneo. En concordancia con lo anterior, Colombia planteó un modelo sistémico basado en objetivos estratégicos que fueron analizados en cada uno de los componentes de carácter cibernético. Para esto fue preciso delimitar y definir prospectivamente hacia dónde deben ir las FF. EE., a fin de desarrollar las capacidades militares que necesiten para realizar operaciones cibernéticas, soportadas en un marco legal y constitucional, así como involucrar todas las capacidades de la organización para ejecutar las OO. EE. en una guerra no convencional.

La importancia de establecer un modelo de ciberseguridad radica en que mejorar sensiblemente la capacidad defensiva y ofensiva de una nación en el ciberespacio le permite controlarlo y aumentar su adaptabilidad, de forma que pueda contar con una ciberfuerza nacional moderna con capacidades diferenciales de carácter estratégico. Así, se podría constituir una organización efectiva y completamente interoperable para emplearla en la defensa y la seguridad de un territorio, con distinción en el quinto dominio de la guerra.

Además, se debe tener en cuenta que el ciberespacio está cambiando rápidamente, de modo que el panorama cultural del mundo desafiará cada vez más los conceptos tradicionales de la sociedad y la identidad nacional. Según Colom et al. (2013), "la conciencia situacional en el ciberespacio conlleva a que una vez se ha alcanzado suficiente nivel de madurez en las técnicas y los medios de ciberdefensa" (p. 90), resulta necesario continuar mejorando y tener la capacidad de conocer, dinámicamente, el nivel de seguridad de los sistemas que se tengan a cargo. De esta manera será posible utilizar de forma adecuada los recursos y aplicar los principios de la gestión de riesgos aprovechando la información sobre las amenazas y usando modelos probabilísticos obtenidos del análisis de los datos de seguridad.

Esta situación de cambio constante exige que los Estados tengan una respuesta inmediata a las amenazas a partir de la información que reciben sobre incidentes de seguridad. Para lograrlo, deben apoyarse en técnicas de visualización de datos complejos que les permitan tomar las decisiones adecuadas en el menor tiempo posible. Asimismo, deben considerar la situación actual de los sistemas de conciencia situacional para ciberdefensa y la importancia que tiene la visualización de la información.

En efecto, según Medina-Ochoa (2019),

la seguridad en el ciberespacio es un desafío para Colombia donde nos presenta un escenario en el cual el Estado debe hacer uso de todos los medios

con que cuenta para preservar sus intereses y logrando proteger no solo su infraestructura crítica con la que cuenta desde el campo de acción de las Fuerzas Militares. (p. 5)

Generar conciencia sobre estas nuevas amenazas en el campo de la ciberseguridad y la ciberdefensa exige la participación de todas las entidades de carácter público, privado y mixto, así como de los sectores académicos, dado que los riesgos pueden escalar y, por lo tanto, impactar gravemente la seguridad del Estado (Miranzo & Del Río, 2014). Consciente de esta situación, en el caso de Colombia, el Consejo Nacional de Política Económica y Social (CONPES) definió las múltiples partes interesadas en el Esquema Nacional de Seguridad Digital (CONPES 3854 de 2016): el Gobierno Nacional y los gobiernos territoriales; las organizaciones públicas y privadas; la fuerza pública; los propietarios u operadores de las infraestructuras críticas cibernéticas nacionales; la academia y la sociedad civil. Estos actores dependen del entorno digital para todas o algunas de sus actividades económicas y sociales, de manera que pueden ejercer distintos roles y tener responsabilidades específicas en las acciones de seguridad digital (CONPES 3854 de 2016).

Como se deduce, mantener el ritmo de desarrollo en este dominio es un desafío para la defensa nacional, pues requiere dedicación, pero también una inversión inmensa de recursos. Por esta razón, es esencial que la capacidad cibernética se implemente como una herramienta en todos los campos de las Fuerzas Militares, lo cual solo es posible con la inmersión, a nivel doctrinaria y de experticia, en el ámbito cibernético (Aguilar-Antonio, 2019). Se debe agregar que a pesar de todos los retos y desafíos descritos, el problema más básico en el dominio cibernético es que no se cuenta con una base conceptual compartida que permita abordarlos, pues la ausencia de terminología, procedimientos y precedentes judiciales internacionales compartidos hace difícil que se establezca una disuasión efectiva. Esta situación se presenta no obstante que el enfoque del mantenimiento de la soberanía y la seguridad estatal ha sido una de las preocupaciones en la agenda política de los países (Guerrero, 2022), dadas las transformaciones que han surgido en el entorno debido a la globalización y la transnacionalización de prácticas como el terrorismo y el narcotráfico, las cuales han deslegitimado las instituciones sociales y políticas. En un escenario de carácter estratégico nacional e internacional, se deben priorizar las amenazas que vulneran el equilibrio, la estabilidad y la seguridad de una nación, así como el sinnúmero de acciones que se pueden realizar en el mundo no físico.

[T1] Retos para las Operaciones Especiales de Colombia: lecciones de la anexión rusa en Crimea

La cuarta revolución tecnológica amplió el espectro de los riesgos y las amenazas de la seguridad y defensa nacionales. Transformó el dominio del ciberespacio e inició la construcción de nuevos escenarios de implementación de estrategias para contrarrestar las acciones del adversario (Medina-Ochoa, 2019). Por ejemplo, los ataques terroristas, cuya intensidad se magnificaba debido a la percepción de inseguridad que producían en la opinión pública, se transforman ahora drásticamente mediante el empleo de las herramientas tecnológicas y las redes sociales. A causa de esto, el ciberterrorismo se ha convertido en un arma de alcance mundial que amenaza sin distinción a los Estados, las organizaciones militares, los emporios empresariales, las entidades bancarias y los individuos (Poveda & Torrente, 2017).

Este fenómeno ha planteado la necesidad de contar con medios seguros para la transmisión de datos (redes seguras). No obstante, la posibilidad de responder efectivamente ante las amenazas que surgen en la guerra cibernética se encuentra con la dificultad de delimitar fronteras y áreas específicas para combatirlas, y con ello, la conciencia de que se trata de una problemática de carácter global ante la cual no es posible contrarrestar todos los riesgos del dominio ciberespacial.

Según Arteaga (2019), “mientras desaparece el orden liberal de postguerra y no acaba de crecer el nuevo orden global” (p. 109), la geopolítica regresa y las grandes potencias utilizan sus instrumentos económicos y tecnológicos para reforzar su capacidad de influencia global. El regreso a la geopolítica se nutre del acelerado proceso de cambio tecnológico en curso, así como de la carrera de las grandes potencias por controlar los nuevos desarrollos tecnológicos y analizar el impacto que tiene la disrupción tecnológica sobre la dinámica de competición geopolítica entre países como Rusia, Estados Unidos y China, actores principales que han desarrollado esta capacidad en operaciones ofensivas y defensivas en el dominio cibernético.

Durante las operaciones militares, los campos de batalla se convierten en zonas fracturadas en las que el nivel de confusión, el ruido y la ambigüedad impactan de forma significativa el cumplimiento de los objetivos operacionales y tácticos. En este escenario, la conciencia situacional (CS) se convierte en un reto porque la percepción de la situación es inestable, lo cual conduce a una comprensión degradada y a la incapacidad del soldado para proyectar los resultados apropiados. Para afrontar estos retos, diversos proyectos militares se han centrado en diseñar sistemas

digitales integrados como soporte para la toma de decisiones del personal, así como en emplear cibersoldados para mitigar el riesgo en el quinto dominio de la guerra.

Además, la incorporación de nuevas tecnologías y medios de comunicación impacta significativamente la toma de decisiones en el orden cibernético. Por ejemplo, en el contexto del conflicto entre Rusia y Ucrania se ha documentado que el General Valeri Vasilievich Guerásimov (Jefe de Estado Mayor de las Fuerzas Armadas Rusas) desarrolló un tratamiento de guerra que emplea instrumentos híbridos y acciones no militares que pueden tener mayor impacto en una zona gris, es decir, una combinación de capacidades para ejecutar las operaciones militares en el desarrollo del conflicto. En la invasión a Crimea (Ucrania) en el año 2014, las Fuerzas Especiales Rusas (los Spetsnaz) fueron protagonistas porque emplearon este tipo de organizaciones especiales en un ambiente de guerra no convencional.

Específicamente, la guerra híbrida es un tipo de enfrentamiento compuesto en el que tiene un papel determinante desestabilizar a una nación, obtener el control de sus recursos y destruir la escala de valores de su sociedad. Con este propósito, se desarrolla una operación de desinformación sin precedentes (Beleño, 2020) que transforma de manera significativa la inclusión de parámetros de FF. EE. a una ciberguerra. En el caso de Ucrania, las Fuerzas rusas emplearon diferentes estrategias que potenciaron la efectividad de la invasión del territorio y la anexión posterior de Crimea a la Federación Rusa.

Según Hoffman (2007), la guerra híbrida consiste en “una amenaza, susceptible de ser utilizada tanto por Estados como por actores no-estatales, que aprovecha toda la gama de modos y estilos de lucha disponibles” (p. 23). En pocas palabras, estas características de la guerra híbrida han sido aplicadas en el conflicto internacional para explotar las capacidades no regulares, motivo por el cual se busca desarticular el sistema agresor con una maquinaria de desinformación, sabotaje y operaciones cibernéticas.

De cualquier modo, lo cierto es que Rusia comprendió en el año 2014 la forma de integrar las capacidades tecnológicas con grupos de FF. EE. y separatistas rusos, con el fin de emplearlos en la invasión de Crimea y en la frontera con ataques cibernéticos. De igual forma, logró atacar mediante capacidades cibernéticas las infraestructuras críticas de la región y así desestabilizar las entidades gubernamentales y bancarias, así como la infraestructura de carácter logístico y ferroviario.

Ahora bien, con el objeto de comprender las capacidades de las FF. EE. rusas en este conflicto y decantar las lecciones aprendidas surgen dos preguntas importantes: ¿Quiénes son realmente los Spetsnaz? ¿Por qué las unidades especiales lograron vincular en sus misiones capacidades cibernéticas?

Los Spetsnaz son una unidad militar conformada el 24 de octubre de 1950 que está compuesta por hombres de FF. EE. de élite, quienes pertenecen a las fuerzas militares y policiales de la Federación de Rusia. Jerárquicamente, pertenecen al Departamento Central de Inteligencia del Estado Mayor de las Fuerzas Armadas. Según García (2022), los Estados Unidos afirmaron que “1500 soldados llamados Spetsnaz eran los responsables de los primeros ataques a Ucrania [...]. Los Spetsnaz son unidades especializadas en misiones de sigilo, sabotaje e infiltración de líneas enemigas” (s. p.). Estas características son perfectas y esenciales para que desarrollen las acciones cibernéticas en contra de sus adversarios, pues les permiten insertarse detrás de las líneas enemigas o mantener un perfil bajo para ejecutar misiones de reconocimiento y vigilancia a largo plazo.

Asimismo, Rusia buscó explotar las herramientas del ciberespacio y reclutó a “corsarios” virtuales y cazarrecompensas para realizar ataques cibernéticos contra la información del gobierno ucraniano. En la dimensión geopolítica y virtualmente incierta que se estaba presentando, los Spetsnaz lograron cambiar su modo de operar. Rusia generó flujos épicos de desinformación, tanto dentro como fuera de Ucrania, no solo para oscurecer la guerra no convencional habilitada cibernéticamente, sino también para crear ilusiones políticas completas. Por lo tanto, no se trataba de desarrollar estrategias de desinformación simples, sino que estuvieran estructuradas de manera compleja y significativa. De acuerdo con esto, las suplantaciones, falsificaciones, mentiras y filtraciones, así como el ciber sabotaje generalmente asociado con la guerra de información, se desarrollaron con antelación para tener la menor resistencia posible.

En ese momento, la desinformación cibernética logró crear un estado de confusión y caos en la población ucraniana. Esto permitió que los ataques cibernéticos ganaran tiempo y espacio para que los Spetsnaz, portadores de equipos computacionales, ejecutaran sus planes en las infraestructuras estratégicas de la región. Adicional es esto, algunas de las características de los “Spetsnaz GRU” fueron determinantes en la actuación de las cibercélulas: equipos de dos soldados o incluso de forma individual que aplican técnicas y tácticas en misiones especiales, lo cual les permite una mayor movilidad y una ágil infiltración en las áreas críticas.

Gracias a todos estos elementos, Rusia cumplió de forma brillante sus objetivos en la operación de ocupación. No solo por la hibridación que hizo de sus capacidades cibernéticas y de FF. EE., sino también porque invadió con éxito una nación socia de la Unión Europea sin provocar ninguna respuesta militar occidental significativa. Cabe señalar que las FF. EE. rusas son protagonistas en las distintas luchas

antiterroristas que se desarrollan en el mundo por las capacidades distintivas que poseen. Estas destacadas características se fundamentan en la calidad de su entrenamiento en asalto e infiltración, operaciones de sabotaje, ciberespionaje y en la desestabilización de blancos, aspectos que convierten a estas unidades en un referente de guerra no convencional y de alta contundencia operacional (Sancho, 2017).

También se debe tener en cuenta que Rusia es una superpotencia en el campo cibernético, con un arsenal importante de herramientas tecnológicas, el cual está acompañado de mercenarios virtuales y piratas informáticos capaces de ejecutar ataques disruptivos y potencialmente destructivos. De igual modo, un análisis más profundo de sus propiedades evidencia que tienen la posibilidad de realizar ataques en paquete, lo cual les permite aprovechar las vulnerabilidades específicas de su adversario.

Este estudio de caso evidencia las capacidades emergentes que las FF. EE. deben desarrollar para afrontar los riesgos y las amenazas cibernéticas en la ofensiva y la defensiva.

Recomendaciones a las Fuerzas Especiales de Colombia en reconocimiento especial y acción directa en un escenario cibernético

Las operaciones de las FF. EE. difieren de las operaciones de unidades convencionales principalmente por los riesgos que asumen y por las técnicas operacionales que emplean para cumplir la misión (Ejército Nacional de Colombia, 2018). Esto significa que cuentan con capacidades distintivas y se focalizan en la sorpresa, la iniciativa y la contundencia. De modo que su efectividad se potencia aún más si a su habilidad se suman las ventajas que brinda el dominio del ciberespacio en la guerra convencional, pues ahora entran en juego como una oportunidad para obtener una ventaja en la batalla contra los adversarios.

No obstante, se debe señalar que existe una serie de factores que afectan el ambiente operacional moderno. El enemigo que “no” está en el ambiente físico, que se encuentra inmerso en un mundo ciber y que ha determinado desarrollar sus actividades mediante una “identidad virtual”, tiene una firma diferenciadora que modifica la forma en que se desarrollan las guerras y las batallas. Por esta razón, la diferenciación responsable del entorno ciberespacial debe garantizar la identificación de las amenazas que abundan en este tipo de dominio.

En consecuencia, los comandantes se deben preguntar: ¿Cómo se deben emplear las capacidades cibernéticas en las OO. EE.?, y, por lo tanto, ¿para qué precisamente se van a emplear? Además, deben observar detenidamente los cambios que se experimentan al tratar de contrarrestar este tipo de amenazas.

Al respecto conviene decir que es necesario observar el comportamiento que adoptan las amenazas internas, las cuales aprovechan adecuadamente las capacidades que les brinda el ciberespacio para fomentar sus acciones criminales. Por ejemplo, existen amenazas en el conflicto armado interno que también emplean las capacidades que ofrece el dominio ciberespacial, como fue el caso de Andrés Felipe Vanegas Londoño, conocido como alias *Uriel* o *Pedro*, quien era el tercer jefe del Frente de Guerra Occidental del Ejército de Liberación Nacional (*El Tiempo*, 2020) y que desarrollaba sus actividades de terrorismo y narcotráfico en el Choco.

A pesar de tener una presencia física en la región, decidió emplear la nube (*web*) como una herramienta de reclutamiento de jóvenes. Instrumentalizando las vías tecnológicas desde el anonimato y la clandestinidad que le brindan las redes sociales, apoyaba económicamente los estudios superiores de jóvenes militantes, a cambio de que cumplieran un plan de trabajo dentro del movimiento social y estudiantil el ELN (*El Tiempo*, 2020). Este tipo de acontecimientos da fuerza a los argumentos de Jaime Blasco, director de los Laboratorios de Seguridad Alien Vault en Silicon Valley, quien asegura que

[...] la guerra cibernética complementa la guerra tradicional y al mismo tiempo refleja el uso y costumbres. También en la guerra cibernética hay soldados y espías: empleados de las fuerzas armadas y los servicios de inteligencia, muchos de ellos reclutados en universidades, pero también en el submundo de hackers delincuentes, dedicados a ejecutar misiones contra intereses de otros países. (Bassets, 2015, p. 14)

Por lo tanto, para analizar este tipo de riesgos y amenazas es fundamental desarrollar conceptos clave que fomenten la estructuración doctrinaria que se necesita para contrarrestarlos, pues seguramente continuarán evolucionando a medida que la tecnología les permita innovar. No obstante, según Vergara y Trama (2017), “en la actualidad no existen definiciones comunes para expresiones relacionadas con la cibernética, ni siquiera en contextos regionales” (p. 21). Por lo tanto, para identificar las capacidades cibernéticas que deben desarrollar las FF. EE. es importante tener en cuenta las doctrinas militares en el campo de la ciberdefensa que han desarrollado países como Estados Unidos, Francia, Dinamarca, Finlandia,

Italia, Israel, Países Bajos, Estonia, España y Brasil, así como los aportes que se pueden extraer de la Organización del Tratado del Atlántico Norte (OTAN) y de la Unión Europea (UE).

Capacidades cibernéticas en las Fuerzas Especiales

En este punto se debe señalar que la idea de integrar las capacidades cibernéticas en las FF. EE. cruza la línea que propuso el Consejo de Seguridad de las Naciones Unidas el 5 de marzo de 2011, que mediante la Resolución N.º 1113 de 2011 hizo un llamamiento a todas las naciones para que cese el desarrollo de capacidades cibernéticas y a repudiar el uso de tácticas de guerra cibernéticas.

Aun así, es menester contar con capacidades cibernéticas diferenciadoras para contener amenazas “simétricas o asimétricas ofensivas y defensivas por parte del Estado” (Vergara & Trama, 2017, p. 37), las cuales puedan tener relación con acceder, interrumpir, destruir, alterar, entre otras acciones, a los actores estatales o interestatales que pongan en riesgo la seguridad y la defensa de la nación.

Educación y cultura ciber

Para Conti y Surdu (2009),

[...] la guerra cibernética requiere no solo de habilidades técnicas, sino también de habilidades para solucionar problemas de creatividad, para actuar de manera equilibrada bajo presión y de pensamiento crítico. Los atributos que son deseables en los soldados, como la resistencia física, la puntería y las habilidades técnicas asociadas con el empleo de las fuerzas tradicionales y sistemas de armas, no se condicen con la guerra cibernética. (p. 17)

Por lo tanto, la capacitación y el entrenamiento de los “ciberguerreros”, como se denominarían en las FF. EE., o en nuestro caso particular “cibercomandos”, deberán ir mucho más allá de habilidades comunes desarrolladas en otros dominios para que puedan ser más contundentes en las misiones de carácter estratégico que ejecutan para la nación (González-Martínez & Montero-Moncada, 2020).

Legitimidad doctrinal en el ambiente cibernético

El uso complejo de estas capacidades debe tener en cuenta el *Manual de Tallin* para implementar de forma legítima y alineada la doctrina en operaciones ciber de FF. EE. Al llegar a este punto se puede indicar que las operaciones de información

en la gran mayoría de los Estados tienen una conexión perfecta, lo cual les permite focalizar el esfuerzo de las FF. EE. y promover otras tantas acciones, de modo que podrían ser el primer acercamiento a una real doctrina de empleo.

Fuerzas Especiales Cibernéticas en el Ejército Nacional

Las operaciones de apoyo de información militar (MISO, por la sigla en inglés de Military Information Support Operations), operaciones de engaño, operaciones de red de computadores (pasivas, activas y de exploración), operaciones de seguridad, la guerra electrónica, las relaciones públicas y las operaciones cívico-militares serían en gran medida la primera fase de desarrollo de unas Fuerzas Especiales Cibernéticas en el Ejército Nacional, pues permitirían a su vez integrar técnicas, tácticas y procedimientos más complejos de lo que se podrían ejecutar en el largo plazo (Espitia et al., 2021). Además,

lograr integrar a una fuerza cibernética en el componente de Fuerzas Especiales del Ejército Nacional permitirá, en las misiones específicas, orientar actividades que tendrán relación con ataques de red de computadoras (CNA), defensa de red de computadoras (CND) y exploración de red de computadoras (CNE), las cuales están contenidas en las operaciones cibernéticas ofensivas, defensivas y de redes de información. (Vergara & Trama, 2017, p. 239).

Capacidad de cibercélulas

Incluir la capacidad de cibercélula a los equipos de reconocimiento de las FF. EE. de Colombia permite un acceso diferenciador en el dominio ciberespacial, lo cual ofrece la oportunidad para que la organización anexe capacidades únicas para el desarrollo de OO. EE. debidamente marcadas en la doctrina colombiana.

Las cibercélulas son, en esencia, una capacidad para la ciberseguridad y la ciberdefensa nacionales (Colom et al., 2013). El trabajo de Colm et al. (2013) muestra que actualmente, salvo países pioneros en ciberseguridad y ciberdefensa como los Estados Unidos, China e Israel, la mayor parte de los Estados está desarrollando sus capacidades cibernéticas básicas, las tecnologías de la información y las comunicaciones, las organizaciones y los procedimientos que las harán funcionar cuando alcancen su madurez. Cuando eso ocurra, será necesario articular las organizaciones y los procedimientos operativos –las cibercélulas– para que operen con esas capacidades. Asimismo, están definiendo el concepto de las cibercélulas,

sus funciones, tareas y ámbitos de actuación, así como los habilitadores que harán posible su funcionamiento (Pons, 2017).

Aunque se trata de una capacidad de siguiente generación y complementaria a las que se están instalando, en el caso de España los autores proponen que es necesario reflexionar sobre el tipo de cibercélulas que complementarían las capacidades de ciberseguridad y ciberdefensa que están desarrollando las Fuerzas Armadas y en las Fuerzas y cuerpos de seguridad del Estado. Sobre todo si se tiene en cuenta que una cibercélula puede ser una eficaz herramienta para que tanto las fuerzas de seguridad como las Fuerzas Armadas de los Estados puedan mejorar la seguridad y la defensa de un determinado ámbito cibernético (Colom et al., 2013).

Finalmente, se debe señalar que las cibercélulas estarían compuestas por equipos operacionales y tácticos que actuarían bajo el control de un mando estratégico cibernético, para la cual requerirían la existencia previa de un conjunto de capacidades de ciberseguridad y ciberdefensa tradicional ya maduras, una infraestructura TIC moderna y un personal experimentado y habituado a operar en este entorno. De esta manera, las cibercélulas podrían conducir operaciones cibernéticas de naturaleza defensiva y ofensiva, apoyarían la evaluación y mejora de las capacidades nacionales, multinacionales o aliadas, al tiempo que permitirían experimentar con nuevos conceptos operativos o adiestrar al personal destinado en esta organización.

Reclutamiento de hackers éticos

En el contexto de este trabajo es importante analizar el reclutamiento de hackers blancos para que trabajen con las FF. EE. en una guerra híbrida, ya sea en un conflicto interno o externo, y comprender completamente el ambiente operacional que se relaciona con las ciberamenazas.

En la actualidad el personal especializado en estas capacidades son en su gran mayoría personas especializadas y expertas en las áreas de la computación, quienes han debido explorar empírica o académicamente los conocimientos necesarios para adquirir dichas habilidades. En algunos casos muy puntuales existen *hacker for hire* ("piratas de alquiler"), que si bien participan en las ciberguerras o en el desarrollo de tecnologías muy precisas, no lo hacen hombro a hombro con las tropas en el terreno. También se encuentra la clasificación o tipo de *hackers* que en el medio académico se clasifican de la siguiente forma: *black hat* ("hacker malicioso"), *white hat* ("hacker ético"), *grey hat* ("no malicioso, pero no muy ético"), *green hat* ("novato"), *blue hat* ("vengativo") y *red hat* ("vigilante").

Por lo tanto, se debe tener en cuenta que el proceso de reclutamiento trae consigo algunas variables negativas que pueden generar consecuencias potencialmente peligrosas para las instituciones de seguridad y defensa, de manera que se requiere de articulación, la cual se focaliza en nuevas transformaciones institucionales.

El Departamento de Operaciones Especiales en el Ciberespacio

Incluir un departamento dedicado a las OO. EE. en el ciberespacio es una prioridad a corto plazo, pues, como se analizó en el apartado anterior, existen riesgos que deberán ser gestionados por una organización lo suficientemente capaz para determinar la doctrina, la organización, el material y el equipo, el personal y la infraestructura (DOMPI) necesarias para estructurar planes concretos en las diferentes actividades que se requieren en el nivel estratégico, operacional y táctico.

Conclusiones

Colombia experimenta una evolución en los conceptos y preceptos doctrinarios de la guerra moderna que obliga a reforzar iniciativas que trascienden las capacidades de seguridad y defensa tradicionales. La influencia de las guerras de sexta generación en los actuales conflictos, como es el caso de Oriente Medio y Europa del Este, está marcando la hoja de ruta en la preparación que deben tener las Fuerzas Militares para contener la expansión de los riesgos y las amenazas en el ciberespacio.

El empleo de las FF. EE. en las OO. EE. incrementa todas las medidas de seguridad antes, durante y después en el planeamiento y la misión, razón por la cual se requiere un sinnúmero de actividades de seguridad que contrarresten su vulnerabilidad.

La implicación y el empleo tanto de las FF. EE. como de las operaciones cibernéticas pueden contribuir significativamente a mejorar la ciberseguridad y la ciberdefensa de la nación, para lo cual se pueden generar células especializadas para la guerra cibernética.

Por lo anterior, este capítulo hace las siguientes recomendaciones a las Fuerzas Militares de Colombia: implementar capacidades cibernéticas en las FF. EE.; generar un modelo de educación y cultura ciber; garantizar la legitimidad doctrinal en el ambiente cibernético; crear unidades de Fuerzas Especiales Cibernéticas en el Ejército Nacional; desarrollar la capacidad de cibercélulas; reclutar hackers éticos y establecer un Departamento de Operaciones Especiales en el Ciberespacio.

Referencias

- Aguilar-Antonio, J. M. (2019). Hechos ciberfísicos: Una propuesta de análisis para ciberramenazas en las Estrategias Nacionales de Ciberseguridad. *URVIO, Revista Latinoamericana de Estudios de Seguridad*, (25), 24-40. <https://doi.org/10.17141/urvio.25.2019.4007>
- Arteaga, F. (2019). Disrupción tecnológica y orden global. *Revista UNISCI*, (51), 109-128. <https://tinyurl.com/mrxnrzst>
- Barbe, E. (1987). El papel del realismo en las relaciones internacionales: Teoría de la política internacional de Hans J. Morgenthau. *Revista de Estudios Políticos*, (57), 149-176. <https://tinyurl.com/mpwzp726>
- Bassets, M. (2015, 8 de febrero). El más fuertes es el más vulnerable: EE.UU. es víctima y, a la vez, el más poderoso agresor en el 'cibertablero' mundial. *El País*. <https://tinyurl.com/mrx756zy>
- Beleño, B. (2020). *Capacidades técnicas, legales y de gestión para equipos BlueTeam y RedTeam* [Trabajo de especialización, Universidad Nacional de Colombia Abierta y a Distancia]. Repositorio UNAD. <https://tinyurl.com/2susm9p9>
- Colom, G. (2012). Vigencia y limitaciones de la guerra híbrida. *Revista Científica General José María Córdova*, 10(10), 77-90. <https://doi.org/10.21830/19006586.228>
- Colom, P., Coz, J., Fojón, E., & Hernández, A. (2013). Las cibercélulas: Una capacidad para la ciberseguridad y la ciberdefensa nacionales. *ARI*, (26), 1-10. <https://tinyurl.com/2p8puuvv>
- Consejo Nacional de Política Económica y Social [CONPES]. (2016). *Política Nacional de Seguridad Digital*, CONPES 3854. Departamento Nacional de Planeación. <https://tinyurl.com/bdzhjvdy>
- Conti G., & Surdu, J. (2009). Army, Navy, Air Force, and Cyber: Is it time for a cyberwarfare branch of military? *A Newsletter*, 12(1), 14-18. <https://tinyurl.com/2bscnp7h>
- Cujabante Villamil, X. A., Bahamón Jara, M. L., Prieto Venegas, J. C., & Quiroga Aguilar, J. A. (2020). Ciberseguridad y ciberdefensa en Colombia: Un posible modelo a seguir en las relaciones cívico-militares. *Revista Científica General José María Córdova*, 18(30), 357-377. <https://doi.org/10.21830/19006586.588>
- Ejército Nacional de Colombia. (2018). *Manual de Campaña del Ejército MCE 318 Operaciones de Fuerzas Especiales [Restringido]*. Imprenta Ejército.
- El Tiempo*. (2020, 25 de octubre) ¿Quién era y cómo operaba "Uriel", el terror del ELN en Chocó? <https://tinyurl.com/shjz4t8x>
- Espitia, A., Agudelo, J., & Ramírez T. (2021). Percepciones sobre innovaciones tecnológicas en el Ejército colombiano. *Revista Logos, Ciencia & Tecnología*, 13(2), 85-102. <https://doi.org/10.22335/rict.v13i2.1408>
- García, B. (2022, 9 de marzo) Las Fuerzas Especiales de Rusia: ¿Quiénes son los Spetsnaz? *Noticiero Televisa*. <https://tinyurl.com/4d4dxhec>

- González-Martínez, M. A., & Montero-Moncada, L. A. (Eds.) (2020). *El tridente del poder estratégico: Inteligencia, Operaciones Especiales y poder ciber en el siglo XXI*. Sello Editorial ESDEG. <https://doi.org/10.25062/9789584288943>
- Guerrero Vallejo, G. Y. (2022). *Operaciones cibernéticas y seguridad hemisférica en Colombia: Análisis desde la cooperación regional e internacional* [Tesis de maestría, Universidad Santo Tomas]. Repositorio USTA. <https://tinyurl.com/2s3s5st3>
- Hoffman, F. (2007). *Conflict in the 21st Century: The rise of hybrid wars*. Potomac Institute for Police Studies. <https://tinyurl.com/dyc5rmnv>
- Junta Interamericana de Defensa. (2020). *Guía de ciberdefensa: Orientaciones para el diseño, planeamiento, implantación y desarrollo de una ciberdefensa militar*. Junta Interamericana de Defensa. <https://tinyurl.com/3k3ttky3>
- Medina-Ochoa, G. (Ed.) (2019). *La seguridad en el ciberespacio, un desafío para Colombia*. Sello Editorial ESDEG. <https://doi.org/10.25062/9789585216549>
- Miguel-Gil, J. (2019). El tratamiento informativo de la guerra híbrida de Rusia. *URVIO, Revista Latinoamericana de Estudios de Seguridad*, (25), 108-121. <https://doi.org/10.17141/urvio.25.2019.4006>
- Ministerio de Defensa Nacional. (2017). Plan Nacional de Protección y Defensa para la Infraestructura Crítica Cibernética de Colombia. <https://tinyurl.com/455ky3f2>
- Miranzo, M., & Del Río, C. (2014). La protección de infraestructuras críticas. *UNISCI Discussion Papers*, (35), 339-352. <https://tinyurl.com/36k8z69t>
- Mitaritonna, A. D. (2019). *Empoderamiento de la conciencia situacional en operaciones militares utilizando realidad aumentada* [Tesis de doctorado, Universidad Nacional de La Plata]. Repositorio UNLP. <https://tinyurl.com/yuz3ucke>
- Nieva, M., & Gazapo, M. (2016). La ciberseguridad como factor crítico en la seguridad de la Unión Europea. *UNISCI Journal*, (42), 47-68. <https://tinyurl.com/mrejyh6a>
- Organización de los Estados Americanos [OEA]. (2019). *Alfabetización y seguridad digital: La importancia de mantenerse seguro e informado*. Organización de los Estados Americanos. <https://tinyurl.com/3nhfztxp>
- Patiño Orozco, G. A. (2019) El sistema internacional cibernético: Elementos de análisis. *Oasis*, (30), 163-186. <https://doi.org/10.18601/16577558.n30.10>
- Pons Gamón, V. (2017). Internet, la nueva era del delito: Ciberdelito, ciberterrorismo, legislación y ciberseguridad. *URVIO, Revista Latinoamericana de Estudios de Seguridad*, (20), 80-93. <https://doi.org/10.17141/urvio.20.2017.2563>
- Poveda Criado, M. A., & Torrente Barredo, B. (2016). Redes sociales y ciberterrorismo: Las TIC como herramienta terrorista. *Opción*, 32(8), 509-518. <https://tinyurl.com/mr3r78tc>
- Realpe, M. E., & Cano, J. (2020). Amenazas cibernéticas a la seguridad y defensa nacional: Reflexiones y perspectivas en Colombia. En V. Gauthier, R. A. Méndez, J. Cano, J. Ramió & L. E. Sánchez (Eds.), *Seguridad informática: X Congreso Iberoamericano, CIBSI 2020* (pp. 105-113). Universidad del Rosario. <https://doi.org/10.12804/si9789587844337.10>

- Sánchez, D. R., & Rodríguez, F. (2010). Seguridad nacional: El realismo y sus contradictores. *Desafíos*, (15), 119-177. <https://tinyurl.com/mu2vbmú6>
- Sancho, C. (2017). Ciberseguridad: Presentación del dossier. URVIO. *Revista Latinoamericana de Estudios de Seguridad*, (20), 8-15. <https://doi.org/10.17141/urvio.20.2017.2859>
- Vergara, E., & Trama, G. A. (2017). *Operaciones militares cibernéticas: Planeamiento y ejecución en el nivel operacional*. Escuela Superior de Guerra Conjunta de las Fuerzas Armadas de Argentina. <https://tinyurl.com/mr3cyap4>

Capítulo 5

Operaciones de Fuerzas Especiales frente a sistemas de amenazas basados en guerra política y guerra de información*

DOI: <https://doi.org/10.25062/9786287602809.05>

Oscar Mauricio Bernal Vallarino

Ilmar Ubiratan Salgado Luzia

Escuela Superior de Guerra "General Rafael Reyes Prieto"

Resumen: La guerra política y de informaciones no son fenómenos nuevos, pero han sido mejor identificados y definidos en el siglo XX, donde han ganado relevancia como medios utilizados por actores estatales y no estatales. Su principal ventaja es la posibilidad de influir en ambientes operacionales, contrarrestar sus adversarios y llevar a cabo sus objetivos sin la necesidad de declaración de guerra formal. En ese contexto, diversos países alrededor del mundo han desarrollado doctrinas de Fuerzas Especiales para poder actuar en áreas de operaciones con el empleo masivo de guerra especial y operaciones de información para ganar el apoyo de las poblaciones, entrenar fuerzas amigas y debilitar el enemigo. En este capítulo se analiza el papel de las Fuerzas Especiales de Colombia, de acuerdo con su doctrina y sus capacidades, en una estrategia para actuar en un ambiente en donde se presentan la guerra política y la guerra de informaciones.

Palabras clave: estrategia; guerra de información; guerra especial; guerra política; operaciones especiales.

* Este capítulo es resultado de investigación adscrito al proyecto "Naturaleza de la guerra contemporánea. Retos y oportunidades de las Fuerzas Especiales y la Inteligencia", adscrito al Departamento Ejército de la Escuela Superior de Guerra, inscrito en la línea de investigación "Naturaleza de la guerra, terrorismo, nuevas amenazas", que forma parte del grupo de investigación Centro de Gravedad, categorizado en A por Minciencias, con código COL0104976. Los puntos de vista pertenecen a los autores y no reflejan necesariamente los de las instituciones participantes.

Oscar Mauricio Bernal Vallarino

Teniente Coronel del Ejército Nacional del Arma de Fuerzas Especiales de Colombia. Magíster en Seguridad y Defensa Nacionales, Escuela Superior de Guerra "General Rafael Reyes Prieto", Colombia. Especialista en Administración de Recursos Militares, Escuela de Armas y Servicios del Ejército Nacional. Profesional en Ciencias Militares, Escuela Militar de Cadetes "General José María Córdova", Colombia. Administrador de Empresas, Universidad Politécnica Grancolombiano. Contacto: oscar.bernalva@buzonejercito.mil.co

Ilmar Ubiratan Salgado Luzia

Teniente Coronel del Ejército del Brasil. Magíster en Seguridad y Defensa Nacionales, Escuela Superior de Guerra "General Rafael Reyes Prieto", Colombia. Posgraduado en Operaciones Militares, Escola de Aperfeiçoamento de Oficiais, Brasil. Ciencias Militares, Escuela de Comando y Estado Mayor del Ejército, y en Inteligencia, Escuela de Inteligencia del Ejército. Licenciado em Ciências Militares, Academia Militar das Agulhas Negras, Resende, Brasil. <https://orcid.org/0000-0002-7680-916X> - Contacto: ubiratan.ilm@eb.mil.br

Citación APA: Bernal Vallarino, O. M., & Salgado Luzia, I. U. (2024). Operaciones de Fuerzas Especiales frente a sistemas de amenazas basados en guerra política y guerra de información. En L. A. Montero Moncada & O. A. Garzón Gómez (Eds.), *Comandos: Retos de las Fuerzas Especiales e Inteligencia en la guerra contemporánea* (pp. 115-140). Sello Editorial ESDEG. <https://doi.org/10.25062/9786287602809.05>

COMANDOS: RETOS DE LAS FUERZAS ESPECIALES E INTELIGENCIA EN LA GUERRA CONTEMPORÁNEA

ISBN impreso: 978-628-7602-79-3

ISBN digital: 978-628-7602-80-9

DOI: <https://doi.org/10.25062/9786287602809>

Colección Seguridad y Defensa

Sello Editorial ESDEG

Escuela Superior de Guerra "General Rafael Reyes Prieto"

Bogotá D.C., Colombia

2024



Introducción

El interés realista que ha generado la guerra tuvo como efecto la apertura de caminos sitiados. En este sentido, se debe establecer que gran parte de las fronteras en el mundo se han establecido mediante grandes enfrentamientos bélicos por disputas territoriales, hecho que se debe a un nacionalismo acuñado con discursos irracionales que masifican al individuo y ponen el bien común por encima del bien individual.

En este contexto, Colombia ha estado sometida por más de medio siglo a una violencia desmedida infringida por los grupos insurgentes, de corte marxista, que se han consolidado en el país basados en un discurso radical. En consecuencia, el país ha sido estigmatizado por un conflicto interno conocido mundialmente.

Las décadas han pasado, las dinámicas sociales y las tecnologías han cambiado en ese período, mientras que el conflicto y sus actores se han adaptado a las nuevas condiciones que impone el nuevo milenio. En este escenario se ha ampliado la importancia que tiene la dimensión informacional, al tiempo que las tecnologías digitales han generado nuevas herramientas para cambiar opiniones y utilizarlas en la guerra.

Para entender ese fenómeno y aplicarlo a la realidad de Colombia es necesario volver a los conceptos de *guerra política*, acuñado por la doctrina de defensa americana en la Guerra Fría, y de *guerra de información*, término surgido en la misma doctrina en la década de 1990.

En este capítulo se analiza si los grupos armados al margen de la ley y sus apoyadores han desarrollado guerra política y guerra de información en Colombia, principalmente en la última década.

Así la cosas, se busca responder esta pregunta orientadora: ¿Cuáles son los retos y las oportunidades de la División de las Fuerzas Especiales (DIVFE) del Ejército

Nacional de Colombia frente a sistemas de amenaza basados en guerra política y guerra de información?

Para cumplir ese objetivo, el capítulo está articulado en tres apartados con objetivos específicos: examinar el empleo de la guerra política y la guerra de información por las amenazas; correlacionar los nuevos requerimientos de los sistemas de amenazas basados en guerra política y guerra de información con el empleo de la DIVFE, y analizar los alcances operacionales y estratégicos de la DIVFE frente a sistemas de amenazas basados en guerra política y guerra de información.

El empleo de la guerra política y la guerra de información por las amenazas

En este apartado se analiza el uso de estrategias de guerra política y guerra de información por las amenazas. Para eso, es importante entender que el concepto de guerra política es más amplio y que comprende diversos tipos de acciones, incluso las operaciones realizadas en un contexto de guerra de información. Dicho de otra forma, la guerra de información es un concepto que está contenido en el espectro de las acciones de la guerra política.

La guerra política

Cuanto más se investiga el concepto de guerra política, resulta más difícil definir una línea de separación entre la política y la guerra. En el siglo XIX, Clausewitz defendió que la guerra se constituía en la continuación de la política con otros medios. A mediados del siglo XX, el diplomático americano George Kennan definió la guerra política como la práctica de la doctrina militar de Clausewitz en tiempos de paz.

Más detalladamente, Kennan argumentó en 1948 que la guerra política podía ser definida como el empleo de todos los medios de que dispone una nación, con la excepción de la guerra, para cumplir sus objetivos nacionales. A partir de esta reflexión se empezó a utilizar el término para definir la estrategia americana aplicada en el período de la Guerra Fría para contrarrestar el avance comunista en el mundo. Las estrategias van desde acciones abiertas, como medidas económicas, alianzas políticas y propaganda “blanca”, hasta acciones encubiertas, como el soporte clandestino a grupos amigos en el exterior, la guerra psicológica “negra” y la promoción de la resistencia popular en Estados hostiles (N. Rodríguez, 2019). Posteriormente,

en un artículo de 1985, Kennan afirmó: "Secreto excesivo, duplicidad y las acciones clandestinas simplemente no son nuestro plato desde que tales operaciones entran en conflicto con nuestras propias normas tradicionales y comprometen nuestra diplomacia en otras áreas" (Lucas & Mistry, 2009, p. 45).

Tal reflexión sobre el aumento de la política exterior de EE. UU. entre 1946 y 1950, trae a colación cuestiones éticas y posibles desventajas diplomáticas en la aplicación del término propuesto por Kennan. Sin embargo, el concepto y su aplicabilidad se volvieron tan efectivos que los análisis posteriores del diplomático americano fueron desconsiderados (Lucas & Mistry, 2009).

A partir de la definición de Kennan se percibe que la guerra política siempre ha existido, pues todos los países han tratado de desarrollar de una forma u otra la política de otros Estados hacia posiciones favorables para sus objetivos (Lucas & Mistry, 2009). A lo largo del tiempo, se pueden encontrar incontables ejemplos de la ejecución de acciones abiertas, encubiertas o mixtas. Del caballo de Troya a los ciberataques, la historia apunta un sinnúmero de ejemplos de interferencia de diferentes estilos (N. Rodríguez, 2019).

Analizando con detalle la naturaleza de las acciones encubiertas, se infiere que se trata de una forma de prevenir una escalada militar con consecuencias desastrosas. Los países que la practican han decidido que es mejor adoptar los supuestos del realismo político y tomar medidas proactivas al respecto. El realismo político hizo de la guerra política el instrumento ideal para practicar la guerra, con estrategias heterodoxas, sin la confrontación directa (N. Rodríguez, 2019).

George Kennan inspiró el programa americano de contención del expansionismo soviético con su concepto de guerra política. El programa proponía medidas económicas y políticas para contrarrestar la esfera soviética, las cuales debían incluir la potencialización de operaciones afirmativas y oportunas con medios encubiertos en la guerra psicológica y económica, destinadas a apoyar y fomentar los disturbios y la subversión en los países que poseían satélites estratégicos. El gobierno delegó la responsabilidad de ejecutar las acciones encubiertas a la Agencia Central de Inteligencia de los Estados Unidos (CIA, por la sigla en inglés de Central Intelligence Agency) (N. Rodríguez, 2019).

Desde entonces, la CIA ha perfeccionado las tácticas y técnicas de la guerra política. Por ejemplo, la campaña que realizó en Chile llevó más de una década, durante la cual las acciones encubiertas financiaron partidos políticos y propagandas en la prensa, además de fomentar abiertamente el golpe de estado militar. En otros casos, como el golpe de estado que realizaron en Irán o las numerosas

operaciones en Siria, han ejecutado actividades similares. Es difícil encontrar un hecho de importancia internacional en el cual la CIA no haya participado de alguna forma. Sus acciones demuestran que implementar la guerra política no es sencillo, pues la diplomacia pública debe estar sincronizada con las acciones encubiertas y las acciones clandestinas (que son las realizadas sin que se informe al Congreso). La guerra política difunde propaganda blanca, gris y negra, crea alianzas con disidentes y promueve acciones subversivas (N. Rodríguez, 2019).

China ha sido otro ejemplo claro de utilización de una estrategia de guerra política. Para China, la guerra política, nombrada por ellos *guerra irrestricta*, es una guerra que lo abarca todo, sin restricciones, como elemento fundamental de la estrategia de seguridad y de su política exterior. Así las cosas, esa estrategia representa para los chinos una alternativa a la guerra violenta, que busca influir en las emociones, los motivos, el razonamiento objetivo y el comportamiento de gobiernos, organizaciones, individuos y grupos de una manera más favorable a los propios objetivos políticos, militares y económicos. La guerra política de China va más allá del tradicional frente único. Su estrategia busca un trabajo de enlace, con el desarrollo de coaliciones para apoyar a la República Popular China y “desintegrar” a los enemigos. Están ahí incluidas las *tres guerras*, que comprenden la guerra de opinión pública y de medios de comunicación, la guerra psicológica y la guerra jurídica. La guerra política de los chinos también involucra medidas activas, tales como la violencia y otros modos de ataques coercitivos y destructivos (Gershaneck, 2020).

Desde la visión china, esa es una guerra librada principalmente por el control y la influencia, para lo cual se emplea la coerción, la corrupción y las violentas operaciones encubiertas. La República Popular China prefiere ganar esta guerra sin tener que disparar nunca un tiro, pero sus cada vez más poderosas Fuerzas Militares y paramilitares se suman en el fondo en apoyo de su creciente guerra de influencia (Gershaneck, 2020).

Por su parte, la guerra política rusa no se centra en eventos aislados, sino que, al contrario, está en el centro de una estrategia política desplegada contra Occidente para debilitar sus instituciones y socavar el consenso transatlántico. Como tal, los esfuerzos de Moscú trabajan en el refuerzo mutuo, aunque no siempre de manera claramente coordinada, como si fuera un ecosistema en evolución. Este complejo ecosistema consiste en una red de actores *proxy*, organizaciones de medios, cuentas de redes sociales, intereses comerciales creados, oligarcas, grupos de la sociedad civil, ciberdelincuentes, agencias de inteligencia, empresas

privadas y actores políticos dentro y fuera de Rusia. Algunos de estos actores actúan a instancias directas del Kremlin, y otros fuera de su propia agenda política, pero con el mismo objetivo final. El sistema es un objetivo en movimiento que evoluciona continuamente en su sofisticación, en su complejidad y en la ocultación deliberada (Polyakova & Boyer, 2018).

Paradójicamente, Moscú también afirma algo similar: sosteniendo su papel civilizador, percibiéndose amenazada y alistando mentalmente a su pueblo para la guerra, también señala que es objeto de una guerra política ejecutada por Occidente. Definida por los rusos como toda acción militar o no-militar (cultural, política, económica, diplomática, informativa o medioambiental) y direccionada a debilitar un adversario y basada en el empleo de organismos no gubernamentales (ONG) y organizaciones civiles, el apoyo a opositores políticos o movimientos sociales, el control de internet y de las tecnologías de la información, la propaganda en los medios de comunicación y la penetración cultural, esta guerra promovida por Estados Unidos pretendería explotar la posibilidad de protesta popular para provocar o facilitar cambios de gobierno en Rusia. La percepción rusa de amenaza y su menor poder militar convencional en relación con la Alianza del Tratado del Atlántico Norte (OTAN) le hace justificar sus actividades de desestabilización y subversión, sus operaciones de información o sus operaciones militares en su área de influencia regional (Piella, 2019).

Desde el punto de vista legal, dentro de los acuerdos que regulan la guerra se encuentran el Estatuto de Roma, los Convenios de Ginebra y la Declaración Universal de los Derechos Humanos. Estos estatutos pretenden de alguna manera generar un marco jurídico y normativo que le diga a los Estados (o diferentes actores involucrados en la guerra) lo que pueden o no realizar a fin de no violar los Derechos Humanos, ni el Derecho Internacional Humanitario. Al analizar la guerra política, se infiere que esos tratados y las leyes internas de los países funcionan como límites en los cuales los actores se basan para establecer sus estrategias y decidir incluso si esos límites serán respetados o desbordados.

En este sentido, Borrero (2017) considera que, en la actualidad, la guerra como intrínsecamente se plantea tiende a ser mal interpretada y su grado de aceptación es justificado en aquello que la motiva. Dicho de otra manera, la guerra se ha llegado a considerar necesaria para defender ideologías o territorios. Esa calificación no se contrapone con la posibilidad de la guerra inevitable o la guerra justificada, lo cual evidencia que el largo debate sobre el concepto de guerra política se termina enmarcando en una errónea guerra justa, pues cada uno de los contendores

expone lo que para ellos son sus razones. Por esta razón, desde un punto de vista más ambiguo, Borrero (2017) no solo describe la guerra política como una potencial respuesta a los intereses de regular un orden mundial, sin que la proscriba como un mecanismo de fortalecimiento entre las disputas de los Estados.

Asimismo, en la Carta de las Naciones Unidas se ha consolidado un avance que se deriva de los mecanismos establecidos en el derecho de hacer la guerra –en adelante *ius ad bellum*– y que intenta entender las razones de los Estados para argumentar la guerra justa y la confusión que deriva de dichas razones. Así, la guerra política termina siendo un método no permitido para hacer la guerra porque no se ha establecido ningún mecanismo para regularla.

En este contexto es fundamental establecer las conceptualizaciones más relevantes sobre la guerra, en las cuales la guerra política encaja dentro de los implementos del poder. La figura 1 presenta una comparación entre conceptos y doctrinas de guerra basados en el empleo de medios estatales o no estatales para cumplir los objetivos políticos de los países.

Figura 1. Comparación del uso de los medios en los diferentes tipos de guerra.



Fuente: Elaboración propia.

Esta comparación permite observar que los conceptos coinciden en la utilización de medios más allá de los convencionales para influir en la política de otros países. La diferencia básica en esa comparación es que la estrategia de guerra política americana no incluía el empleo de elementos criminales o fuerzas terroristas como medios para llevar a cabo las acciones. Los conceptos de guerra híbrida y guerra irrestricta sí lo hacen. Así las cosas, se puede inferir que la guerra irrestricta, desde el punto de vista de los medios, es un tipo de guerra política según la

doctrina de China. En el caso de la guerra híbrida, si bien en la doctrina americana se excluyen otros instrumentos del poder nacional, diversos teóricos los incluyen, lo que la haría parecerse a una vertiente de guerra política o guerra irrestricta. Hay que comprender los períodos y las condiciones en los cuales se crearon esos conceptos, así como que no hay consenso sobre ellos. Sin embargo, lo importante en esa comparación es percibir cómo los límites legales y éticos restringen los medios empleados en las estrategias y se pueden cambiar en los aspectos determinantes de “nuevos” tipos de conflicto.

Cabe resaltar que en la anterior ilustración se puntualizan cuatro aspectos fundamentales en la guerra política, entre los cuales se incluye la diplomacia, que puede ser utilizada para prevenir potenciales enfrentamientos bélicos o para azuzarlos si se llegara el caso. Así se evidenció durante la Guerra Fría, pues pese a que se suele definir como un enfrentamiento no bélico, los contendores, que en ese caso eran EE. UU. y la URSS, se enfrentaron en diferentes escenarios, como la península de Corea, Vietnam, Alemania, entre otros.

Asimismo, se destacan las operaciones militares, pues aunque algunas incluso tienen objetivos de mantenimiento de paz, terminan generando tensión entre los Estados y promoviendo una guerra que rápidamente podría pasar de ser política a un enfrentamiento bélico.

Guerra de información

La guerra de información es la doctrina contemporánea de carácter no oficial creada en la década de los años 90, cuyo planteamiento principal es el empleo de la información como arma en el combate armado y en la confrontación política, para la defensa o toma del poder (Tovar, 2011). Consiste en la utilización de la información con el fin de obtener una ventaja sobre el oponente. La guerra de la información puede constituirse en la recolección de información táctica, confirmación de la veracidad de la información propia, en distribuir propaganda o desinformación para desmoralizar al público y al enemigo, en reducir la eficiencia de la información enemiga y en negar oportunidades de recolección de información (Rojas et al., 2011). Además, puede trabajar en el sentido de ganar el apoyo de grupos o poblaciones en un área de operaciones.

Como ya se ha dicho, la guerra de información está incluida en las acciones que un actor puede emprender en el contexto de la guerra política, de manera que no se debe entender como una herramienta distinta, sino como un complemento. Sin embargo, las acciones de guerra de información no se perciben solamente

como complemento de las operaciones militares, pues pueden ser ejecutadas como un curso de acción independiente (Tovar, 2011).

La guerra de información altera y ataca los sistemas epistemológicos del enemigo para generarle confusión en la distinción de lo real y, de esa forma, disminuir la eficiencia del proceso para la toma de decisiones y cumplir el objetivo (Tovar, 2011). Con ese propósito, se hace una difusión masiva de ataques informativos dirigidos a los blancos audiencias con narrativas que apuntan a debilitar los adversarios, fundamentalmente a través de la radio, la prensa, la televisión y la internet. Esto implica además la ejecución de tácticas o la emisión de opiniones que, a través de su difusión mediática y cobertura, alteren los conocimientos y las creencias de los adversarios, así como su percepción de la realidad. Estas acciones hacen necesario, entonces, un grado de coordinación entre los operadores civiles de los servicios informacionales y el comando militar (Tovar, 2011).

La dependencia del ser humano para representarse la realidad a partir de los medios se convierte entonces en una ventaja fundamental que posee el agresor informacional para cumplir sus objetivos. En el esquema de guerra de información es factible y justificable la difusión masiva de mentiras, la desinformación o *fake news* y la generación de confusión y miedo en la población. Así, la ejecución de operaciones de información por medio de los medios incorpora estrategias no violentas de guerra en la vida cotidiana, disipando la distinción entre la paz y la guerra (Tovar, 2011).

Empleo de la guerra política y la guerra de información por las amenazas en Colombia

La transformación del conflicto interno en Colombia ha hecho que los Grupos Armados Organizados (GAO) cambien sus estrategias, sumando nuevos elementos a su guerra de guerrillas. Su estrategia para influir las poblaciones y públicos audiencia ha incluido a veces el cultivo de aliados políticos en el exterior y campañas de desinformación. Sin embargo, dado que la guerra política, por definición, es emprendida tan solo por actores estatales, hay que mirar holísticamente para percibir cuáles son las amenazas que puede emplear la estrategia en contra de nuestro país.

Para llevar a cabo la guerra política, los Estados emplean múltiples capas de *proxies*, que son agentes y entidades directas o indirectas, para mantener la

negación plausible y la ambigüedad estratégica (Polyakova & Boyer, 2018). En ese orden de ideas, los grupos armados organizados, así como las organizaciones criminales, no serían los perpetradores sino los agentes por medio de los cuales un Estado hostil podría poner en práctica su estrategia de guerra política.

Así, un país podría desarrollar la infiltración en Colombia a través de las élites, los partidos políticos, las organizaciones de fachada, los influenciadores y los grupos al margen de la ley. A partir de entonces, podría ejecutar acciones a través de las élites, atomizar y neutralizar las organizaciones políticas y sociales, e incluso hacer un cambio de gobierno. Hoy en día, nada es más sospechoso que operaciones subversivas espontáneas o dispositivos mediáticos con una narrativa directa y unidireccional, teniendo en cuenta la inmensa gama de actores e intereses involucrados (N. Rodríguez, 2019).

Otro método es la identificación de vulnerabilidades sociales por medio de la amplificación de los problemas sociales divisivos. En Latinoamérica la polarización política, la ideología de género, la “lucha de clases”, las cuestiones étnicas y religiosas son amplificadas con el fin de desestabilizar los gobiernos y posibilitar cambios favorables a las amenazas. En los Estados Unidos, la máquina de desinformación de Rusia se ha centrado en las tensiones raciales, la política de justicia penal, la inmigración de personas provenientes de países latinoamericanos y musulmanes, así como en las divisiones de clase (Polyakova & Boyer, 2018).

Para identificar qué actores internacionales de hecho emplean la guerra política en contra de Colombia basta contestar a la pregunta: ¿Qué países emplean medios diplomáticos, informacionales, económicos y militares, con acciones abiertas y encubiertas, para influir en Colombia además de apoyar las acciones de los GAO (ostensiva o veladamente), con el posible empleo de otros medios (narcotráfico, contrabando o inmigración)?

Efectos de la guerra política y de información en las operaciones de FF. EE.

En Colombia, los grupos al margen de la ley han buscado deslegitimar las acciones de las Fuerzas Militares para debilitarlas y restringir su libertad de acción. En ese sentido, esos grupos y sus apoyadores han empleado estrategias discursivas y políticas de ataque a la triada compuesta por las FF. EE., el poder de los ataques aéreo-estratégicos y la Inteligencia. Esta triada se ha convertido en el principal

instrumento de numerosas Fuerzas Militares para confrontar exitosamente a los enemigos asimétricos. Esa herramienta, que hubiera sido invencible en el campo de batalla, es una de las fortalezas de las Fuerzas Militares y puede ser percibida por la amenaza como el centro de gravedad que se debe derrotar mediante la manipulación de la propaganda y la política (Montero, 2021).

La amenaza asimétrica comprendió que si desactivaba en parte su componente armado para enfocarse en medios de presión social, política y jurídica, no solo podría debilitar algunas capacidades del Estado que tendrían la posibilidad de derrotarla en el campo de batalla, sino también controlar una narrativa utilizando una opinión pública cambiante en redes sociales (Montero, 2021). De acuerdo con las narrativas, las acciones legítimas de Inteligencia son en la realidad acciones de persecución política y abuso contra la privacidad; los ataques aéreos estratégicos empleados en el marco del Derecho Internacional Humanitario (DIH) son abusos contra el propio DIH. Asimismo, el Ejército pierde gradualmente su libertad de acción a partir de la guerra jurídica perpetrada en su contra, la cual hace que los militares sean judicializados por abusos en el simple cumplimiento de sus tareas constitucionales. Así, es importante considerar que la guerra política librada deviene del reconocimiento de la incidencia que tienen los factores políticos en la actividad militar, aspectos que debían ser ampliamente atendidos por el Ejército Nacional (Rojas, 2017).

En consecuencia, tal cual sucede desde la antigüedad, delante de la imposibilidad de enfrentar a un ejército más fuerte o la oportunidad y voluntad de no hacerlo, el adversario utiliza estrategias asimétricas, se confunde entre las poblaciones, evalúa como centro de gravedad la población adversaria, actúa ajeno a los usos y costumbres de la guerra, aprovecha para sus intereses el DIH e intenta que sus actividades obtengan efectos estratégicos mediante una eficaz explotación informativa de sus actos lógicos, físicos e informativos. Es decir, la amenaza explota las debilidades morales, políticas, sociales, demográficas, jurídicas, económicas o militares de adversarios más eficaces en el enfrentamiento directo (Piella, 2019).

En este escenario, también se debe tener en cuenta que el ámbito tecnológico desarrolló las telecomunicaciones, la informática y los medios audiovisuales o mediáticos, lo cual impactó el orden económico, político y cultural, especialmente a partir del hito que representó internet en la comunicación e interdependencia de los países. Esto aceleró la unificación de mercados, los movimientos de capital y la creación de nuevas comunidades, que superaron las sociedades y culturas existentes (Piella, 2019).

Con el desarrollo de las tecnologías de la información y las comunicaciones, se han creado redes sociales digitales que han revolucionado las relaciones interpersonales y la manera de sostener conversaciones en la actualidad. La facilidad y comodidad proporcionada por la tecnología en multitud de campos ha permitido que esta permee ámbitos educativos, empresariales y gubernamentales, en campos donde se puede vulnerar la percepción de los colombianos, especialmente porque su introducción facilitó actividades cotidianas y promovió otras que años atrás eran consideradas imposibles (M. C. Rodríguez, 2019).

Por lo tanto, la revolución de la información viene siendo comparada con la Revolución Industrial, en la medida en que supuso un salto histórico y social gracias a la aplicación masiva de la tecnología en los procesos productivos, aunque ahora esa tecnología no es la máquina de vapor, sino el acceso a la información (M. C. Rodríguez, 2019). En ese sentido, se hace necesario aprovechar la velocidad de los cambios que tienen las tecnologías, pues ellos ofrecen herramientas claves para apoyar el proceso de toma de decisiones, la protección y la letalidad, pero con la consciencia de que su empleo correcto incluye la utilización del dominio cibernético y de la dimensión informacional.

Dado el carácter multidimensional de la seguridad cibernética en Colombia, se hace necesario implementar herramientas para dar continuidad al proceso de ciberresiliencia y de obtención de los objetivos y estrategias, apoyándose en un diagnóstico situacional.

Es más, el futuro presentará nuevos retos, pues los avances de tecnología en inteligencia artificial, el aprendizaje automático y la automatización, sumados al creciente uso de *big data*, han preparado los escenarios para una nueva era de guerra política, económica y de alto impacto. A corto plazo, será más difícil, si no imposible, diferenciar entre audio, video o personalidades en línea reales y falsificadas, de manera que se hace más arduo distinguir entre informaciones confiables o no. Los actores maliciosos utilizarán estas tecnologías para atacar a las sociedades de manera más eficaz y eficiente. A medida que Estados como Estados Unidos, Rusia y China inviertan recursos en el desarrollo de tecnologías, la competencia global por el próximo salto en la guerra política se intensificará. Así las cosas, el análisis prospectivo indica que las estrategias necesitan no solo mitigar las amenazas actuales, sino también las futuras, en un contexto en que las oportunidades para hacerlo se están agotando rápidamente (Polyakova & Boyer, 2018).

La ejecución de acciones de desinformación requiere el uso de actores clave manifiestos y encubiertos. La amenaza puede utilizar sus medios informacionales

estatales y, asimismo, los medios encubiertos podrían ser *trolls* de redes sociales, cuentas automatizadas (*bots*), cuentas de suplantación de identidad en Facebook, Twitter (ahora X) e Instagram, o sitios de internet (Polyakova & Boyer, 2018).

Considerando el apoyo internacional que reciben los grupos al margen de la ley, desde el punto de vista de la guerra política se puede inferir que el empleo de estructuras *proxy* caracterizaría el uso de esos grupos con el objetivo de desestabilizar el ambiente político interno. En tal orden de ideas, este fenómeno político-económico generó la necesidad de analizar, especificar y comprender cómo funcionaba la guerra política en países de América Latina, a tal punto que incluso se ha convertido en uno de los desafíos más importantes para los académicos del momento.

Para poder determinar las afectaciones y los roles de las FF. EE. frente a estos retos es importante dar un vistazo a los otros Estados que se han visto sometidos por la guerra política, haciendo hincapié en las consecuencias políticas, económicas y sociales que se presentaron durante estos gobiernos.

Los países con gobiernos dictatoriales buscan tener la capacidad de controlar la opinión pública por medio del control de los medios de comunicación. Al mismo tiempo aplican restricciones y censura a contenidos informacionales como sitios de internet, músicas y películas que, dentro de su evaluación, podrían perjudicar sus objetivos políticos y estratégicos. Así, la coacción de las libertades personales es una herramienta que los gobiernos dictatoriales suelen utilizar en nombre de un supuesto bien mayor colectivo que la justificaría. Esto se puede ver claramente en el caso del sandinismo en Nicaragua, donde el Estado

[...] impuso una ley de excepción que restringía las libertades públicas; aplicó una ley de medios que censuraba a la prensa independiente; creó organizaciones sociales que en lugar de luchar por sus gremios defendía las políticas del partido sandinista aún en detrimento de sus propias necesidades; se creó un sistema de vigilancia en los barrios que observaba cada movimiento de la gente y si criticaban al gobierno revolucionario eran acusados de contras. (Cisneros, 2014, p. 235)

Esta es la forma en que la guerra política suele relacionarse con la limitación de las libertades personales. En muchos de los casos, tales como el del gobierno de Nicaragua, con el sandinismo, la libertad de expresión se veía coartada, las libertades públicas ya no existían y la prensa era fuertemente controlada, e incluso se veían afectadas las decisiones de vida de las personas.

Por otro lado, los países que practican las democracias representativas al estilo occidental, en donde se busca garantizar libertades individuales como la libertad

de expresión y de pensamiento, son más vulnerables a las campañas de guerra de información de actores internos y externos. En esos países, muchas veces el Estado no tiene las estrategias ni, en consecuencia, las herramientas para contrarrestar esas campañas.

Inspirada en la doctrina militar internacional, principalmente la doctrina OTAN, Colombia ha desarrollado capacidades de OO. EE. para combatir a los GAO. Su evolución, a lo largo de las últimas décadas, llevó a la creación de la DIVFE, que se ha constituido en un comando de OO. EE. encargado de entrenar a sus miembros en acción directa, guerra irregular y recopilación de inteligencia en campos de batalla y en varios dominios, con la responsabilidad de planear y ejecutar las OO. EE. dentro y fuera del territorio nacional (Ejército Nacional de Colombia, 2018b). Con el paso del tiempo, las operaciones que ha ejecutado la DIVFE han tenido un papel fundamental en el éxito de la respuesta estatal a la amenaza de los GAO en Colombia.

Sin embargo, en el marco de las OO. EE., los cambios en la opinión pública interna y la presión internacional; el riesgo de los daños colaterales; la sumisión a usos y costumbres de la guerra anacrónicos y restrictivos; la ansiedad por los efectos electorales y los costes políticos de las acciones operativas; la exigencia de restringir su impacto, alcance y duración, y la necesidad de usar la fuerza de manera restrictiva y limitada son componentes que pueden ser explotados por los actores que contrarrestan un ejército occidental (Piella, 2019). La falta de libertad de acción resultante para emplear los medios de Inteligencia y realizar ataques de precisión quirúrgica tiene efectos debilitantes sobre las operaciones especiales.

Rol de las FF. EE. en las acciones para contrarrestar la guerra política y de información adversarias

Para los americanos, los instrumentos del poder nacional incluyen, además de las dimensiones diplomática, económica y militar, un componente informacional. Ese elemento permite que los planeadores estratégicos tomen consciencia sobre la importancia de que existan estrategias nacionales para informar e influir audiencias en el ambiente externo e interno de un país. Además de servir como medio para buscar la superioridad de la narrativa en la dimensión informacional, esas estrategias sirven como protección a los ataques informacionales de las amenazas, pues generan estructuras especializadas en ese tipo de acciones.

Claramente, el caso americano demuestra que el Estado necesita opciones entre la intervención militar y la no intervención completa. Para darle solución a las amenazas contemporáneas, el Estado debería ser capaz de librar una guerra política con el uso de medidas abiertas y encubiertas, desde acciones económicas, alianzas políticas y propaganda, hasta operaciones encubiertas, guerra psicológica e incluso el fomento de la resistencia clandestina en Estados hostiles (Boot & Doran, 2013).

De acuerdo con la doctrina americana, si bien la estrategia para ejecutar acciones encubiertas efectivas está muy desarrollada, es importante saber la diferencia entre la información y la propaganda: la información para los aliados es la diplomacia pública, mientras que la información para el enemigo es la guerra psicológica (N. Rodríguez, 2019). De ahí se infiere de qué manera funciona la guerra política en el escenario internacional, que es practicada por los países que buscan influir en otros con base en sus justificaciones y, al mismo tiempo, deslegitimar la guerra política adversaria.

En lo que se refiere a las OO. EE., el Ejército americano posee una escuela específica para la educación y el entrenamiento de la guerra especial: la Escuela de Guerra Especial John F. Kennedy. En esa institución el enfoque del entrenamiento ha cambiado poco desde su creación en 1952, que consiste en seleccionar y educar al personal de las FF. EE. para organizar, entrenar y emplear una fuerza guerrillera. En la época de su creación, los conflictos de baja intensidad eran frecuentes y con ellos surgió la necesidad de desarrollar capacidades especiales de guerra: la contrainsurgencia y la guerra no convencional (Department of the Army, 2014).

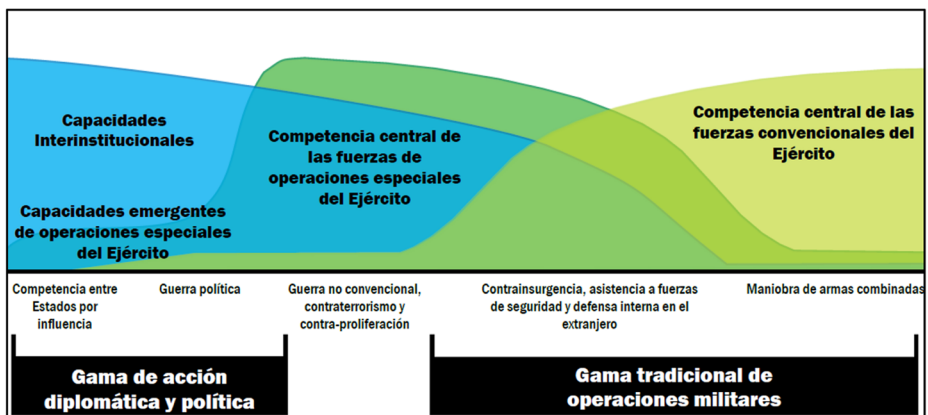
Durante las décadas de 1980 y 1990, la defensa americana reactivó las FF. EE. para responder a las amenazas que se presentaban en las naciones de la cuenca del Pacífico, en el Caribe y en el continente africano. Esas FF. EE. desempeñaron un papel fundamental en el combate de los movimientos guerrilleros y en la contención de la propagación del comunismo en América Central y del Sur, mediante la potencialización de las capacidades militares de los regímenes democráticos. Con este propósito, las FF. EE. fueron desplegadas en El Salvador para desarrollar una fuerza de contrainsurgencia efectiva, ayudar a los hondureños a resistir y derrotar una invasión de Nicaragua y una insurgencia apoyada por los comunistas. Durante la segunda mitad de 1980, las OO. EE. americanas apoyaron acciones de antinarcóticos en Venezuela, Colombia, Ecuador, Perú y Bolivia (Department of the Army, 2014).

La génesis de las FF. EE. en los Estados Unidos ocurrió cuando desarrollaron los conjuntos de habilidades necesarias para una guerra especial. Posteriormente, las capacidades de guerra especial fueron clave para un renacimiento de la guerra

no convencional después del ataque terrorista a las Torres Gemelas el 11 de septiembre de 2001. En esa ocasión, los destacamentos operativos cumplieron un papel central en la derrota de los afganos durante la operación “Enduring Freedom”, en la cual el entrenamiento de insurgentes en contra de los talibanes ganó prominencia con imágenes de “soldados a caballo”. La operación “Irak Freedom” también mostró cómo un pequeño número de equipos de FF. EE., vinculados con el entrenamiento y la ayuda a la resistencia indígena, podrían apoyar grandes operaciones de combate, pues evitaron que trece divisiones iraquíes reforzaran las unidades que defendían Bagdad (Department of the Army, 2014). Esa estrategia de guerra especial con uso de guerra no convencional, en la cual los Estados Unidos emplearon las FF. EE. para potencializar las fuerzas *proxy*, puede ser empleada tanto en la guerra política como en apoyo a las operaciones convencionales.

En un libro blanco del Comando de Operaciones Especiales americano, *Redefining the Win (Redefinir la victoria)*, publicado en 2015, se describe el espectro de conflicto que representa la figura 2. Usando dicho espectro, en ese libro blanco se presenta la guerra no convencional en un campo gris que no encuadra la guerra política ni tampoco de modo preciso la guerra en sí (Linnemann, 2016). A partir de esa imagen se puede concluir que las “capacidades emergentes” y la “competencia central de las Fuerzas de Operaciones Especiales” están comprendidas en el espectro de la guerra política junto a la “gama de acción diplomática y política”. Asimismo, se observa que la guerra política está en algún punto entre la “competencia entre Estados por influencia” y las acciones de guerra no convencional.

Figura 2. Comparación entre capacidades nacionales y de operaciones especiales en relación con el espectro de los conflictos.



Fuente: Linnemann (2016).

De acuerdo con la doctrina de las OO. EE. de Colombia, las operaciones de guerra especial ejecutadas por las FF. EE. incluyen guerra no convencional, asistencia a fuerzas de seguridad, contrainsurgencia, preparación del ambiente operacional, defensa interna en el extranjero, operaciones psicológicas y asuntos civiles, es decir, se asemeja a lo que se describió sobre la doctrina americana (Ejército Nacional de Colombia, 2018b). Todo eso debería indicar que las FF. EE. de Colombia están capacitadas para ejecutar ese tipo de operaciones, pero la práctica revela que esas tropas no han desarrollado esas capacidades, pues han enfocado sus operaciones solamente en ataques de precisión quirúrgica (Sánchez & Alexis, 2020).

La doctrina colombiana de OO. EE. resalta que la defensa interna en el extranjero consiste en la coordinación de las participaciones de las agencias militares y civiles de un gobierno, en cualquiera de los programas de acción adoptados por otra organización o gobierno con la misión de liberar y proteger su sociedad de la subversión, la anarquía, la insurgencia, el terrorismo y otras amenazas a la seguridad. Eso incluye esfuerzos de apoyo para el entrenamiento de fuerzas militares de otros países teniendo en cuenta sus amenazas internas.

En ese contexto, el papel principal de las Fuerzas de Operaciones Especiales debe ser entrenar, asesorar y asistir a las fuerzas de seguridad de la nación anfitriona en una actividad de guerra especial. Según los manuales doctrinales, esto implica un enfoque integral, el cual incluye todos los instrumentos de poder nacional diplomático, informacional, militar y económico. Cabe notar en esa parte la herencia de la doctrina de guerra política americana, como ya se ha establecido (Ejército Nacional de Colombia, 2017).

La defensa interna en el extranjero se ejecuta entonces a través de una acción unificada que implica la sincronización, la coordinación y la integración de actividades de entidades gubernamentales y no gubernamentales dentro de la operación para lograr la unidad de esfuerzo (Ejército Nacional de Colombia, 2017), lo cual denota la importancia de los otros instrumentos del poder nacional, más allá del militar, para llevar a cabo esa estrategia. Sin las acciones coordinadas y el soporte del Estado, las FF. EE. no serán capaces de poner en práctica la guerra especial necesaria para potencializar sus acciones delante de la guerra política adversaria (Paddock, 1980).

La doctrina de OO. EE. destaca todavía la necesidad de que las FF. EE. se preparen en un ambiente operacional antes de que actúen en misiones directas. Es decir, las unidades tienen que cambiar las condiciones que existen actualmente en los ambientes hostiles para debilitar la amenaza, obtener el máximo de informaciones

sobre esta y ganar el apoyo de las poblaciones locales. En ese sentido, las FF. EE. deben conducir la preparación del ambiente operacional como un tipo de actividad de configuración de otras misiones que se prevea conducir en el futuro (Ejército Nacional de Colombia, 2017). Si se aplica correctamente esa capacidad, las FF. EE. podrían conducir sus operaciones con la potencial disminución de los riesgos asociados con la guerra política que libra la amenaza en el territorio nacional. Además, permitiría poder influir en el interior de un Estado agresor para desestabilizarlo por medio del entrenamiento, el asesoramiento y la asistencia a fuerzas de combate locales.

Las tareas de guerra especial no son sencillas. Todo lo contrario, implican que las unidades deben tener la capacidad de operar dentro de una población específica, de manera que deben abordar los factores socioculturales mediante la comprensión de su cultura. En la medida en que el éxito de cualquier operación o campaña militar dependa de la aplicación de capacidades únicas diseñadas para combatir y vencer en conflictos centrados en la población, los factores socioculturales serán parte esencial de las actividades de guerra especial (Paddock, 1980). En este sentido, las OO. EE. deben considerar la totalidad de los aspectos físicos y los entornos sociales y culturales que influyen en el comportamiento humano, pero para eso los operadores especiales necesitan tener una rígida educación y entrenamiento en esos temas (Ejército Nacional de Colombia, 2017).

Cabe destacar que las operaciones de contrainsurgencia exitosas se enfocan en la población, debido a la importancia que tiene crear condiciones de legitimidad y credibilidad para el Gobierno y sus programas. De la misma manera, el apoyo de la población también es un objetivo fundamental para la insurgencia, de manera que debe ser dirigida como parte de un esfuerzo de contrainsurgencia integrado (Department of the Army, 2014).

De acuerdo con la doctrina colombiana, el objetivo de las operaciones de guerra no convencional es lograr un cambio en el control político y la legitimidad percibida de los regímenes. Por lo tanto, se admite doctrinalmente que la guerra no convencional tiene utilidad estratégica, pues puede alterar el equilibrio de poder entre los Estados soberanos. Realizar ese tipo de operaciones conlleva un riesgo político significativo en los ámbitos políticos, tanto nacionales como internacionales, y requiere que su ejecución y supervisión sean delicadas. La necesidad de operar con una mezcla variada de medios clandestinos y encubiertos, maneras y fines, pone de relieve que es fundamental contar con una excelente inteligencia del área en la que se llevan a cabo las operaciones. Como en todos los escenarios de conflicto,

en guerra no convencional las Fuerzas Militares deben coordinar estrechamente sus actividades con los interlocutores interorganizacionales a fin de permitir y salvaguardar operaciones sensibles (Ejército Nacional de Colombia, 2017).

La doctrina de Colombia presenta las operaciones de información como una capacidad distintiva de las FF. EE., la cual ejecuta a través de los niveles estratégicos, operativos y tácticos de la guerra. Además, la doctrina apunta que esas operaciones son también una capacidad del Ministerio de Defensa Nacional (MDN), utilizada como parte de las actividades interinstitucionales para alcanzar los objetivos nacionales (Paddock, 1980). En ese punto, la doctrina americana sobre emplear el instrumento informacional del poder nacional para distinguir sus objetivos tiene eco en los documentos colombianos. Sin embargo, el Estado colombiano no tiene esa capacidad estructurada como ocurre con los Estados Unidos y otros países que la emplean, lo cual hace que la doctrina actual pierda su embasamiento (Department of the Army, 2014).

Doctrinalmente, las operaciones de información son la principal capacidad de información de las FF. EE., pues les permiten analizar y abordar los factores psicológicos en el ambiente operacional; proporcionar apoyo a las actividades de información e influencia como una capacidad básica de las FF. EE.; apoyar a otros organismos de información en influencia; llevar a cabo actividades de operaciones de información en apoyo de autoridades civiles nacionales; suministrar apoyo a la desinformación del adversario; proporcionar un efecto no letal importante para distinguir blancos de alta retribución; conducir operaciones de engaño; influir y conducir la adquisición de blancos; analizar los blancos audiencia dentro del ambiente operacional, y analizar los medios de comunicación en el ambiente operacional (Ejército Nacional de Colombia, 2017). Esta capacidad de las OO. EE. debería coordinar todas las capacidades informacionales existentes en una Fuerza para contrarrestar la guerra de información adversaria. Al respecto cabe mencionar que si bien la doctrina de la OTAN ya tiene el cajón de herramientas desarrolladas y testadas en ambientes operacionales complejos para solucionar los desafíos de la guerra en la dimensión informacional, aún es necesario conocerlas, dominarlas y aplicarlas (Paddock, 1980).

Es evidente que la doctrina de operaciones de información, función esencial de las FF. EE., no está siendo ejecutada en el contexto de las OO. EE. en Colombia como se indica en la doctrina de la OTAN. Al contrario, las FF. EE. colombianas se involucran tan solo en los ataques de precisión quirúrgica, mientras que las unidades o equipos de Acción Integral cumplen el objetivo de influir audiencias, pero con

las limitaciones inherentes a esa especialidad. De ese modo, la DIVFE se aleja de las tareas fundamentales doctrinales de las operaciones de información.

En ese sentido, la DIVFE de Colombia debe identificar, junto con sus agencias de inteligencia, todo tipo de operaciones de desinformación que quieran vulnerar la seguridad y la defensa del país, y que pueden provenir de cualquier tipo de organización o grupos virtuales que tengan como objetivo ejecutar algún plan para desestabilizar la estructura del Estado. Con el cumplimiento efectivo de esta tarea, la DIVFE puede además asesorar de manera oportuna los escalones superiores para el planeamiento estratégico y la definición de política.

Finalmente, hay que tener claro que las actividades de las Fuerzas Militares se deben basar en una serie de reglamentos y leyes, los cuales están sujetos a las normas prescriptivas que rigen la elección de los blancos, y que únicamente se orientarán contra objetivos militares. En ese sentido, se debe enfatizar en que el estricto cumplimiento del DIH, del Derecho Internacional de los Derechos Humanos (DIDH) y de las normas internacionales que rigen los conflictos suministra la legitimidad integral de las operaciones.

Una de las características fundamentales de la guerra de información y de la guerra política es que el Estado debe movilizar todos sus recursos –infraestructura, tecnología y comunicaciones– para acabar con una amenaza que busca constantemente desestabilizarlo. En este sentido, el dominio del Estado debe ser absoluto, pues la amenaza hace un esfuerzo continuo e incansable para ganar las mentes de los ciudadanos.

De acuerdo con Montero (2021), las guerras actuales son asimétricas o híbridas, en la medida en que plantean diferentes desafíos estratégicos, operacionales y tácticos, al igual que la lucha en ambientes operacionales totalmente nuevos y complejos. En este escenario toman relevancia las metodologías de selección de los centros de gravedad, las cuales plantean que en estos novedosos escenarios de confrontación el centro principal del esfuerzo debe direccionarse a la legitimidad o en general a algún factor dentro del espectro de lo político. Así las cosas, es posible afirmar que el objetivo político de la guerra tiene un impacto importante en el objetivo militar, ya que sus efectos pueden desestabilizar el Estado. Por lo anterior, Montero (2021) afirma que el binomio política-guerra está determinado por la capacidad de la Fuerza, la cual se evidencia en los escenarios asimétricos. Evidentemente, una de las principales armas que usa el enemigo en este tipo de guerras es la sensibilidad social, la cual produce un rencor social debido a la desinformación o la mala interpretación de las situaciones.

Conclusiones

La supervivencia de las organizaciones en la historia humana depende de su capacidad para adaptarse al entorno en que operan y del grado de eficiencia que imprimen a sus procesos. Por eso las iniciativas de innovación en materia de seguridad deben generar la adaptación a un entorno cada vez más exigente (Lesaca, 2018).

En este sentido, se concluye que las FF. EE. se han centrado en ejecutar operaciones de precisión quirúrgica para desestructurar y debilitar los grupos armados organizados. Si bien este tipo de acciones ha sido el fundamento de las Fuerzas Militares durante mucho tiempo, los ataques alternativos que generan la guerra política y la guerra de información evidencian la importancia creciente que ha adquirido la guerra especial en el ámbito de las OO. EE., con la convicción de que esos tipos de operaciones tienen la capacidad de influir y cambiar los ambientes operacionales.

Así las cosas, es importante que los operadores especiales se involucren en temas de gran complejidad, como las relaciones entre los gobiernos, las poblaciones y sus culturas, la adaptación a las circunstancias cambiantes, las teorías de victoria y las múltiples dimensiones del entorno en que se desarrolla la formulación de la estrategia.

En este sentido, para la DIVFE es importante identificar las políticas que le faciliten el tratamiento de datos y la información sensible, así como las capacidades informacionales de las que depende la infraestructura estatal. De esta manera puede satisfacer sus necesidades operacionales para cumplir su misión aplicando correctamente los marcos legales.

En ese orden de ideas, la DIVFE ya no puede enfocarse totalmente en el dominio terrestre en el contexto de una fuerza conjunta, sino que además debe proporcionar apoyo a otras fuerzas militares en sus dominios y dimensiones para que puedan superar sus desafíos operativos. Esto quiere decir que el cambio se debe enfocar en potenciar la capacidad de la DIVFE para producir efectos multidominios y en integrar eficaz y continuamente toda la fuerza conjunta (Brown, 2018).

Es la guerra especial y no las operaciones de ataque quirúrgico lo que caracteriza a las FF. EE. en el mundo y las distingue de otras tropas con capacidades similares, como las que poseen los equipos de OO. EE. de la Policía o las Fuerzas de Comando. Un país no puede abstenerse de desarrollar esas capacidades sin pagar el precio de ser más vulnerable a la guerra política adversaria.

Por supuesto, el proceso que le permitiría a Colombia potenciar la capacidad informacional del Estado como instrumento del poder nacional no nace en las FF. EE., sino en su política y estrategia de defensa. Sin eso, las FF. EE. seguirán debilitadas porque no tienen la libertad de acción que necesitan para maximizar sus operaciones, pues la doctrina de la OTAN por sí misma no garantiza que se aplique de forma similar a como se hace en los países desarrollados.

En un país latinoamericano, a veces la privacidad individual suele estar en un grado superior de prioridad en relación con la estabilidad nacional. Al considerar los límites que se imponen a la Inteligencia, mientras que al mismo tiempo se permite el empleo masivo de *fake news* y desinformación, hay que discutir hasta dónde de las libertades individuales se pueden sobreponer al bienestar de la sociedad. La posibilidad de que las campañas de desinformación puedan quedar impunes debido a las políticas de privacidad ha provocado inestabilidades que perjudican a un gran número de personas y que ponen en riesgo la democracia en nuestro país.

La fragilidad de la opinión pública es directamente proporcional al bajo nivel de conocimientos de la población en el tema, lo cual ha servido al enemigo como una herramienta para fortalecerse. Así, haciendo uso de la sensibilidad de la comunidad, logra generar miedo y en algunos casos repulsión hacia la fuerza pública, lo cual evidencia la necesidad de fortalecer los mecanismos de las FF. EE. ante la guerra política y de información. En este orden de ideas, se puede afirmar que la falta de conocimiento en el tema azuza la sensibilidad social.

Así las cosas, es importante recalcar la responsabilidad del Estado en promover mecanismos que permitan mitigar de manera efectiva las amenazas que generan la guerra política y la guerra de información. Para esto es fundamental establecer un pensamiento estratégico en todas aquellas instituciones que ostentan el poder estatal, de tal manera que se pueda contrarrestar con contundencia un eventual ataque.

Finalmente, se debe puntualizar que también es un compromiso del Estado evidenciar los ataques mediáticos a la fuerza pública, así como las potenciales amenazas, pues fortalecer la Inteligencia estratégica sería una herramienta realmente efectiva para evitar dichos ataques. Este fortalecimiento se debe fundamentar en una colaboración institucional que involucre de manera directa a todas las instituciones comprometidas con la seguridad nacional.

Referencias

- Boot, M., & Doran, M. (2013, 28 de junio). Department of Dirty Tricks: Why the United States needs to sabotage, undermine, and expose its enemies in the Middle East. *Foreign Policy*. <https://tinyurl.com/377f5ewf>
- Borrero Mansilla, A. (2017). *Guerra, política y derecho*. Editorial Universidad El Bosque.
- Brown, R. B. (2018). La región del Indo-Asia Pacífico y el concepto de batalla multidominio. *Military Review*, (primer trimestre), 81-88. <https://tinyurl.com/3m36v9xc>
- Cisneros, I. (2014). *Norberto Bobbio: De la razón de Estado al gobierno democrático*. Instituto Electoral y de Participación Ciudadana del Estado de Jalisco. <https://tinyurl.com/4vtdxtxd>
- Colom, G. (2019). La amenaza híbrida: Mitos, leyendas y realidades. *Boletín IEE*, (13), 669-682. <https://tinyurl.com/2y57tjb3>
- Department of the Army. (2014). *Field Manual FM 3-18 Special Forces Operations*. Headquarters, Department of the Army. <https://tinyurl.com/yn6h6atz>
- Ejército Nacional de Colombia. (2017). *Manual Fundamental del Ejército MFE 3-05 Operaciones Especiales [Público]*. Imprenta Militar del Ejército. <https://tinyurl.com/2p8b7nse>
- Ejército Nacional de Colombia. (2018a, 13 de septiembre). Caballería. <https://tinyurl.com/5e3d9yce>
- Ejército Nacional de Colombia. (2018b). *Manual de Campaña del Ejército MCE 3-18 Operaciones de Fuerzas Especiales [Restringido]*. Imprenta Ejército.
- Gershaneck, K. K. (2020). *Political warfare: Strategies for combating China's plan to "win without fighting"*. Marine Corps University Press. <https://tinyurl.com/yc49pkfr>
- Hoffman, F. (2007). *Conflict in the 21st Century: The rise of hybrid wars*. Potomac Institute for Police Studies. <https://tinyurl.com/dyc5rmnv>
- Lesaca. (2018). La disrupción digital en el contexto de las guerras híbridas. *Cuadernos de Estrategia*, (197), 159-196. <https://tinyurl.com/3cxzsaw5>
- Linnemann, R. A. (2016). El arte no convencional y la guerra moderna. *Military Review*, (julio-septiembre), 30-39. <https://tinyurl.com/3xwx5nby>
- Lucas, S., & Mistry, K. (2009). Illusions of Coherence: George F. Kennan, U.S. Strategy and political warfare in the early Cold War, 1946-1950. *Diplomatic History*, 33(1), 39-66. <https://tinyurl.com/mpb8rb95>
- Montero, L. A. (2021, 18 de marzo). De la guerra política como parte de la guerra asimétrica. Escuela Superior de Guerra. <https://tinyurl.com/5u6h86bm>
- Paddock, A. H. (1980). *Psychological and unconventional warfare, 1941-1952: Origins of a "special warfare" capability for the United States Army* [Individual Study Project, US Army War College]. Repositorio DTIC. <https://tinyurl.com/37wsnfnk>
- Polyakova, A., & Boyer, S. P. (2018). *The future of political warfare: Russia, the West, and the coming age of global digital competition*. The Brookings Institution. <https://tinyurl.com/cjsu5mvs>

- Rodríguez, M. C. (2019). *Límites legales del control parental en las redes informáticas con relación al libre desarrollo de la personalidad en niños menores de 14 años* [Trabajo de grado, Universidad Católica de Colombia]. <https://tinyurl.com/yc7vv67s>
- Rodríguez, N. (2019, 7 de noviembre). Guerra política y teoría de las acciones encubiertas 2.0. <https://tinyurl.com/27553jca>
- Rojas Guevara, P. J. (2017). Doctrina Damasco: Eje articulador de la segunda gran reforma del Ejército Nacional de Colombia. *Revista Científica General José María Córdova*, 15(19), 95-119. <https://doi.org/10.21830/19006586.78>
- Rojas, W. A., Benavides, J. F., & Bello, J. C. (2011). Las operaciones de información en las guerras de información [Trabajo de especialización, Universidad Piloto de Colombia]. Repositorio Unipiloto. <https://tinyurl.com/3f7vpwer>
- Sánchez, M., & Alexis, D. (2020). Transformación de las Fuerzas Especiales de acuerdo con la doctrina internacional. *Brújula Semilleros de Investigación*, 4(7), 46-57. <https://tinyurl.com/2xb9xxes>
- Tovar, H. L. (2011). *Guerra de información: ¿El arma es el mensaje?* [Tesis de maestría, Universidad Central de Venezuela]. Repositorio UCV. <https://tinyurl.com/nhhxt9jx>

Capítulo 6

Guerra especial: de la táctica a la práctica^{*}

DOI: <https://doi.org/10.25062/9786287602809.06>

Jorge Rafael Gutiérrez Oliveros

Luis Alexander Montero Moncada

Escuela Superior de Guerra "General Rafael Reyes Prieto"

Resumen: El objetivo de este capítulo de investigación es determinar la importancia de las operaciones de defensa interna en el extranjero y de la guerra no convencional como Operaciones de Fuerzas Especiales dentro del contexto de las guerras contemporáneas. Inicialmente, se define el concepto de guerra especial como capacidad crítica de las Operaciones de Fuerzas Especiales y se describen los conceptos de dos operaciones específicas, las cuales forman parte de la capacidad crítica de la guerra especial: la defensa interna en el extranjero y la guerra no convencional. Posteriormente, se analizan las ventajas que tiene el desarrollo de este tipo de Operaciones de Fuerzas Especiales, para lo cual se toma como ejemplo, de forma general, algunas operaciones de guerra especial desarrolladas por otros países como parte de una estrategia nacional. Finalmente, se analizan los efectos de estas operaciones en los conflictos contemporáneos.

Palabras clave: capacidad crítica; conflictos contemporáneos; estrategia; Fuerzas Especiales; guerra especial.

^{*} Este capítulo es resultado de investigación adscrito al proyecto "Naturaleza de la guerra contemporánea. Retos y oportunidades de las Fuerzas Especiales y la Inteligencia", adscrito al Departamento Ejército de la Escuela Superior de Guerra, inscrito en la línea de investigación "Naturaleza de la guerra, terrorismo, nuevas amenazas", que forma parte del grupo de investigación Centro de Gravedad, categorizado en A por Minciencias, con código COL0104976. Los puntos de vista pertenecen a los autores y no reflejan necesariamente los de las instituciones participantes.

Jorge Rafael Gutiérrez Oliveros

Teniente Coronel del Ejército Nacional del Arma de Fuerzas Especiales de Colombia. Profesional en Ciencias Militares, Escuela Militar de Cadetes "General José María Córdova", Colombia. Especialista en Conducción y Administración de Unidades Militares, y especialista en Administración de Recursos Militares para la Defensa Nacional, Escuela de Armas y Servicios. Instructor invitado en USAJFKSWCS. Contacto: gutierrezjr@esdeg.edu.co

Luis Alexander Montero Moncada

Doctorando en Estudios Políticos, Universidad Externado de Colombia, y en Estudios Políticos y Relaciones Internacionales, Universidad Nacional de Colombia. Magíster (honoris causa) en Inteligencia Estratégica, Escuela de Inteligencia "Brigadier General Ricardo Charry Solano", y en Análisis de Problemas Políticos, Económicos e Internacionales Contemporáneos, Instituto de Estudios Políticos de París Sciences-Po, Universidad Externado de Colombia y Ministerio de Relaciones Exteriores de Colombia. Politólogo con énfasis en Relaciones Internacionales, Universidad Nacional de Colombia.

<https://orcid.org/0000-0003-3420-0863> - Contacto: luis.montero@esdeg.edu.co

Citación APA: Gutiérrez Oliveros, J. R., & Montero Moncada, L. A. (2024). Guerra especial: De la táctica a la práctica. En L. A. Montero Moncada & O. A. Garzón Gómez (Eds.), *Comandos: Retos de las Fuerzas Especiales e Inteligencia en la guerra contemporánea* (pp. 141-162). Sello Editorial ESDEG. <https://doi.org/10.25062/9786287602809.06>

COMANDOS: RETOS DE LAS FUERZAS ESPECIALES E INTELIGENCIA EN LA GUERRA CONTEMPORÁNEA

ISBN impreso: 978-628-7602-79-3

ISBN digital: 978-628-7602-80-9

DOI: <https://doi.org/10.25062/9786287602809>

Colección Seguridad y Defensa

Sello Editorial ESDEG

Escuela Superior de Guerra "General Rafael Reyes Prieto"

Bogotá D.C., Colombia

2024



Introducción

La naturaleza cambiante de la guerra obliga a pensar en el camino idóneo para gestionarla. En ese contexto, las Fuerzas Especiales (FF. EE.) se perfilan como un componente protagonista en el planeamiento y el desarrollo de operaciones militares en un rango cada vez más amplio de enfoques y usos.

Si bien recientemente han aparecido nuevos conceptos que tratan de identificar las diferentes clases de guerra que se presentan en nuestros tiempos, hay tres factores centrales que están relacionados con las nuevas definiciones de "guerra": la diversificación de la amenaza, la multidimensionalidad de los conflictos y la evolución constante de las tecnologías de información. Actualmente no hay un consenso que establezca una definición universal sobre la guerra, sino que existen varios significados que definen actividades diferentes: guerras mundiales, guerra religiosa, guerra asimétrica, guerra híbrida, guerra convencional, guerra irrestricta, entre otras. Específicamente, para efectos de este capítulo, se toma como referencia la definición de guerra de Clausewitz, para quien es un acto de violencia destinado a obligar a los adversarios a cumplir con la propia voluntad.

En este contexto, también existen varios enfoques para clasificar las guerras, como el de las generaciones evolutivas, que

[...] busca enmarcar la guerra dentro de una serie de particularidades que son repetitivas, indistintamente del lugar o región del mundo en donde se esté desarrollando la confrontación armada, pero que a su vez permiten observar elementos distintivos dentro de una generación y otra. Esta teoría tiene sus fundamentos en dos variables: la primera de ellas se enfoca en la tecnología, que puede ser entendida como los medios a través de los cuales se lucha en

una guerra en particular; y la segunda variable la constituye la estrategia, o mejor aún, la teoría de la guerra que se esté empleando en la confrontación armada. (Álvarez, 2017, p. 156)

A pesar de estos enfoques y la variedad de definiciones, el problema de fondo es responder a la pregunta sobre cuál es el medio más adaptativo, flexible y eficaz para enfrentar las amenazas y situaciones de peligro que surgen en estas nuevas guerras. Acá las FF. EE., en función de sus capacidades diferenciales, ofrecen una respuesta importante.

Las FF. EE. del Ejército Nacional han demostrado ser una capacidad determinante dentro de la estrategia del Comando General de las Fuerzas Militares de Colombia (CGFM). Para el señor Mayor General Carvajal, “el empleo de las unidades de FF. EE. ha contribuido al cumplimiento de los objetivos estratégicos de la política de seguridad y defensa nacional” (Ejército Nacional de Colombia, 2017a, p. 14). La doctrina de las FF. EE. en Colombia ha sido desarrollada a partir del conocimiento adquirido a través de la doctrina de otros países, más la experiencia obtenida durante el desarrollo del conflicto interno. Desde esta perspectiva doctrinal, “las Operaciones Especiales son acciones militares conducidas por unidades organizadas, entrenadas, equipadas y certificadas; con alta movilidad y flexibilidad, en espacios hostiles, negados y políticamente sensibles, para alcanzar objetivos militares de repercusiones estratégicas” (Ejército Nacional de Colombia, 2017a, p. 1-3).

Por esta razón, el objetivo de este capítulo es estudiar sus capacidades críticas y analizar cuáles de ellas son idóneas para enfrentar escenarios híbridos. A manera de hipótesis de trabajo, se tiene que la guerra especial, específicamente con las tareas de guerra no convencional y defensa interna en el extranjero, son las herramientas que más y mejor perspectiva ofrecen al respecto.

El capítulo está dividido en cuatro partes. En la primera, se delimitan las capacidades que tienen las FF. EE. para comprender su valor en un universo cambiante de la guerra y en las operaciones militares contemporáneas. En la segunda, se ahonda en el análisis de la guerra especial como factor no solo diferencial, sino, en este caso, también protagónico para enfrentar escenarios híbridos. En la tercera, se estudian las tareas que desde la guerra especial concentran la mayor gama de opciones: la guerra no convencional. En la cuarta parte, se continúa con el estudio

de la defensa interna en el extranjero, como una de las tareas que componen la capacidad de guerra especial idónea para confrontar entornos complejos e híbridos. Por último, se concluye reuniendo lo más representativo del estudio.

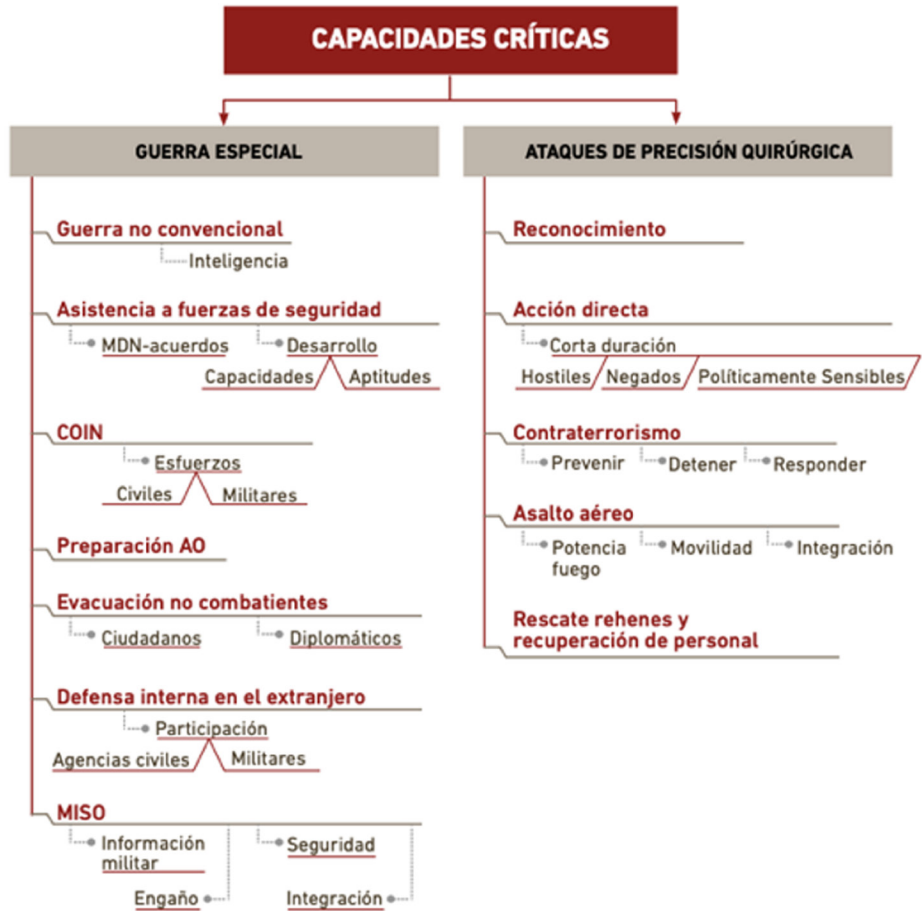
Delimitación de las capacidades de las Fuerzas Especiales, un universo cambiante

El Ejército Nacional de Colombia es un referente en la región debido a su capacidad de hacer la guerra en diferentes ambientes operacionales. En ese contexto, y con más énfasis durante las dos últimas décadas, se han dado las más importantes acciones contra las estructuras irregulares que han operado en el país. En ese sentido, es posible afirmar que “la estrategia gubernamental” y “la acción del Ejército, fortalecido por el Plan Colombia, inclinó la lucha contrainsurgente a favor del Estado” (González & Betancourt, 2018, p. 18), de manera que se logró degradar el centro de gravedad operacional y estratégico insurgente. En este proceso, resulta fundamental destacar la estrategia que empleó el Ejército Nacional para transformar sus FF. EE. y convertirlas en un factor potenciador de las operaciones militares en todo el territorio nacional.

Con el concepto de Operaciones Terrestres Unificadas (OTU), adoptado en 2015, se construyó el sendero para que, doctrinalmente hablando, las Operaciones Especiales (OO. EE.) fueran una de las tres competencias distintivas de la acción decisiva (Rojas, 2017). Es por ello que se delimitaron los conceptos generales de las FF. EE., los cuales quedaron plasmados en el *Manual Fundamental del Ejército MFE 3-05 Operaciones Especiales* (Ejército Nacional de Colombia, 2017a).

El marco de partida para analizar las operaciones de defensa militar desde el extranjero lo ofrece justamente el *MFE 3-05*. En él se distinguen las OO. EE. de las operaciones convencionales porque son conducidas específicamente para cumplir con los objetivos de más alto nivel trazados por la estrategia militar nacional (figura 1). Por su misión, las OO. EE. se pueden desarrollar a través de dos capacidades críticas claramente distintivas frente a fuerzas convencionales: los ataques de precisión quirúrgica y la guerra especial, la cual es el objeto central del presente capítulo.

Figura 1. Capacidades críticas de las Fuerzas Especiales.



Fuente: Ejército Nacional de Colombia (2017c).

Desde el punto de vista doctrinario, la guerra especial está compuesta por siete actividades, las cuales implican “la capacidad de operar dentro de una población específica, para abordar los factores socioculturales mediante la comprensión de la cultura de esta población” (Ejército Nacional de Colombia, 2017b). No obstante, el espectro de la guerra especial sigue siendo un campo sumamente amplio y no existe reglamento, manual o algún tipo de texto que encuadre especialmente a la guerra no convencional. Esta condición puede tener cuando menos dos explicaciones. En primer lugar, posiblemente el énfasis operacional necesario en tareas contrainsurgentes siguió las pautas doctrinarias estadounidenses –con génesis en la contrainsurgencia británica–, en las cuales el esfuerzo principal recaía en adecuar

las unidades convencionales antes que en llevar las FF. EE. a fondo. En segundo lugar, porque al ubicar el concepto de guerra no convencional en el espectro de la guerra especial, la aleja de las tareas más recurrentes pertenecientes a los ataques de precisión quirúrgica.

Incluso, la vaguedad conceptual de la guerra no convencional está presente en la doctrina. Si bien es cierto que el *MFRE 3-05* define este tipo de operaciones como “las actividades conducidas en un ambiente de conflicto, orientadas a la búsqueda de inteligencia para debilitar la capacidad de lucha del adversario en aproximación indirecta, a través de acciones tendientes a limitar sus recursos y capacidades críticas” (Ejército Nacional de Colombia, 2017b, p. 1-14), esta acepción se queda corta respecto a la realidad e importancia de la guerra no convencional, especialmente en el desarrollo de la guerra híbrida.

Y es que se puede considerar a la guerra no convencional como todo un arte, donde “el espacio negativo entre la guerra y la paz es el lugar en donde los actores luchan guerras modernas de manera no convencional, tales como las actividades en el dominio cibernético realizadas por el grupo de hackers” (Linnemann, 2016, p. 36). La definición de Linnemann (2016) en efecto considera un problema de gran trascendencia. La complejidad de los ambientes operacionales contemporáneos, sumada a una sociedad globalizada donde los dominios de la guerra son cada vez más variados e interconectados, hacen difícil definir cuál es el ambiente operacional para lo no convencional o, en otras palabras, dónde se ubica la línea divisoria entre lo convencional y lo no convencional.

Por ello existen múltiples enfoques desde los cuales se puede hacer un acercamiento a las operaciones de guerra no convencional –evidentemente ninguno completo–, que sin embargo coinciden en destacar sus características para maximizar las ventajas operacionales dentro de un ambiente híbrido. Este desafío estratégico es especialmente importante para las grandes potencias, como es el caso de los Estados Unidos, que, según Linnemann (2016), tiene el gran reto de “innovar, adaptar y adoptar la guerra no convencional a través de un amplio planteamiento estratégico, en lugar de sostener su perspectiva actual de una capacidad táctica para una misión especializada” (p. 38).

En esencia, la guerra no convencional es una combinación de aplicaciones directas e indirectas del poder nacional con el propósito de dar cumplimiento a un objetivo estratégico, el cual, por sus características, requiere de una operacionalización especial. “La guerra no convencional del siglo XXI traduce la estrategia nacional y la política en un concepto operacional, que brinda a los hacedores de

política nacional una opción política estratégica, apropiada y rentable” (Department of the Army, 2013, p. 23).

Es así como el Comandante del Comando de Operaciones Especiales del Ejército de los Estados Unidos (USASOC, por su sigla en inglés) precisa que la guerra no convencional es “el conjunto de actividades dirigidas a posibilitar el desarrollo de un movimiento de resistencia para coaccionar, alterar o derrocar a un gobierno o a tomar el poder mediante el empleo de una fuerza clandestina, en un territorio enemigo” (Department of the Army, 2010, p. 14). De esta manera, los esfuerzos deben estar “dirigidos a explotar las vulnerabilidades psicológicas, económicas, militares y políticas de un país adversario, para desarrollar y sostener las fuerzas de la resistencia y cumplir los objetivos estratégicos” (Department of the Army, 2010, p. 14).

Es importante destacar que la guerra no convencional no tiene relación conceptual o doctrinaria directa con las operaciones militares que se realizan en el extranjero o posiblemente llamadas *operaciones encubiertas*, las cuales son el objeto del capítulo. Justamente por la vaguedad del concepto, la guerra no convencional no se limita doctrinalmente a una determinada serie de acciones, sino que aprovecha la zona gris donde se ubica para planear y ejecutar la más amplia gama posible de operaciones de alto impacto, que trascienden las limitaciones de las operaciones convencionales.

Así las cosas, es posible proponer que la diferencia conceptual radica en que las operaciones encubiertas son una técnica más de la guerra no convencional, o explicado de otro modo, la guerra no convencional es el concepto táctico, mientras que las operaciones encubiertas formarían parte de las diferentes y variadas técnicas del desarrollo de la guerra no convencional.

Usualmente las operaciones encubiertas son relegadas al conjunto de acciones posibles de la Inteligencia militar, especialmente en cuanto operaciones de nivel estratégico que se realizan sobre todo en el extranjero. Como resulta evidente, la limitación conceptual aparece cuando se entiende a las operaciones encubiertas solo como el ejercicio de infiltración de una estructura criminal, pero el concepto de *interferencia* amplía decididamente la definición inicial de operaciones encubiertas y la lleva al nivel estratégico.

En ese sentido, las acciones de interferencia que desarrolla un Estado no solo se pueden asociar a las herramientas de poder estratégico –al lado de la negación de área, la disuasión o la obligación–, sino que además tienen como objetivo influir en las condiciones de seguridad, lo cual podría conducir a un compromiso

militar considerable o extendido, o en otras palabras, a neutralizar una amenaza (Rodríguez-Álvarez & Montero-Moncada, 2022).

Sin embargo, dada la actualización de los retos operacionales, la conjunción entre las FF. EE. y la Inteligencia invita a que se vaya más allá de una simple sinergia y se encamine a una fusión más ambiciosa de capacidades. En ese sentido, los modelos de fusión estadounidenses y rusos proponen que las operaciones estratégicas en ambientes externos dan muchos mejores resultados, al tiempo que mantienen la simpleza y la seguridad de la operación de una forma bastante más robusta y eficaz que en el pasado (Montero et al., 2020).

Es por ello que el rango de las operaciones encubiertas se debe ampliar e incluir una serie de capacidades antes reservadas solamente a la Inteligencia. Evidentemente, a nivel doctrinal esto ofrece dos retos cuando menos. Por un lado, generar doctrina donde no hay doctrina. Por otro, emparentar dos conceptos que, aunque amplios, son diferentes: el de *operaciones encubiertas* y el de *defensa militar desde el extranjero*. Para ello, el mejor marco analítico común es la diada guerra especial –como capacidad crítica– y guerra no convencional –como tarea–.

La guerra especial como capacidad crítica de las FF. EE.

Si se parte del hecho de que una capacidad crítica es “un medio considerado como facilitador crucial para que un centro de gravedad funcione y es esencial para el cumplimiento de objetivos impuestos o deducidos” (Ejército Nacional de Colombia, 2017b, p. 2-2), se puede afirmar que las OO. EE. tienen dos capacidades críticas: la guerra especial y los ataques de precisión quirúrgica. Específicamente, “la guerra especial es la ejecución de actividades que implican una combinación de acciones, letales y no letales, llevadas a cabo por tropas que cuentan con un amplio entendimiento y comprensión del ambiente operacional” (Ejército Nacional de Colombia, 2017b, p. 2-2).

En la construcción doctrinaria nacional, la capacidad de guerra especial está constituida por los siguientes tipos de operaciones distintivas: “Guerra no convencional, asistencia a fuerzas de seguridad, contrainsurgencia, preparación del ambiente operacional, evacuación de no combatientes, defensa interna en el extranjero, apoyo a operaciones de información y asuntos civiles” (Ejército Nacional de Colombia, 2017b, p. 2-3).

Su importancia estratégica dentro del contexto de las OO. EE. se basa en que proyecta a las FF. EE. en el nuevo escenario de la guerra híbrida, un claro concepto occidental donde se pueden ubicar muchos de los conflictos contemporáneos y que encuentra definiciones homologables en Rusia –como guerra no lineal– y en China –como guerra irrestricta–. Esta guerra se puede definir como el “producto natural de la adaptación de la guerra irregular y asimétrica encaminada a explotar las vulnerabilidades de las fuerzas regulares” (Colom, 2018, p. 38) o, en el escenario de la guerra irrestricta, se podría definir como “una guerra combinada que trasciende las principales áreas y métodos de los asuntos militares y no militares, donde se deben incluir todas las dimensiones que ejercen influencia sobre la seguridad nacional” (Ejército de Chile, 2013, p. 4) y de esta forma se pretende alcanzar, por medio de la violencia, un objetivo político.

Dicho en otras palabras, en el contexto de la guerra híbrida, la guerra no convencional –como parte de la capacidad crítica de la guerra especial– tiene un papel muy importante. En este sentido es fundamental entender la definición de guerra híbrida:

La guerra híbrida es una sofisticada forma de lucha característica de la Era de la Información que, fundamentada en las posibilidades que brinda la globalización y el libre acceso a las tecnologías avanzadas, se distingue por la combinación, en todos los niveles y fases de la operación, de acciones convencionales e irregulares. (Colom, 2012, p. 82).

Una tercera definición que evidencia la cercanía entre la capacidad de guerra especial y la guerra híbrida es aquella que la define como “el uso de diversos instrumentos de poder que actúan atacando sobre un actor social determinado. Ese uso de las herramientas de poder se convierte en un ataque que busca identificar distintas vulnerabilidades para causar efectos varios” (Equilibrium Global, 2020, párr. 4). Justamente por el carácter difuso a la hora de enfrentar el poder del adversario híbrido es que la guerra no convencional y la defensa interna en el extranjero son centrales y le permiten al Estado entrar en el terreno esquivo de la proactividad, en lugar de estar atados a una reacción permanente.

La guerra especial –y las tareas que la componen– adquiere por tanto protagonismo. Para el Ejército de los Estados Unidos, “las dos misiones (operaciones) primarias son la guerra no convencional y la defensa interna en el extranjero” (Department of the Army, 2014, p. 14). La escogencia de este camino se basa en que son las herramientas más potentes que pueden emplearse para contener enemigos asimétricos, en primera medida –adaptativos, flexibles y difusos–, como

enemigos híbridos, en segunda medida –de confluencia de poder convencional y medios no atribuibles, pero altamente desestabilizadores–. En este punto, se vuelven importantes la guerra no convencional, en la cual los operadores especiales llevan a fondo su flexibilidad y adaptabilidad a entornos operacionales difusos, y la defensa interna en el extranjero, en su carácter preventivo y manteniendo las amenazas lo más lejos posible del territorio.

Dado que el concepto de guerra híbrida es el formato más extendido de la guerra contemporánea (Montero, 2022), es clave que los ejércitos, empezando por el colombiano, hagan un profundo análisis de sus capacidades –en el marco de la guerra especial– respecto al desarrollo de tácticas, técnicas y procedimientos que permitan a las FF. EE. colombianas asegurar la victoria de un conflicto sin siquiera haber disparado la primera bala.

Asimismo, se deben analizar los diferentes aspectos en los cuales la guerra especial puede ser aplicada ante cualquier adversario, entendiendo que el ambiente operacional de la guerra híbrida es sumamente cambiante. La guerra especial desarrollada a través de la guerra no convencional y la defensa militar en el extranjero es un componente militar sumamente importante para la estrategia nacional gubernamental en los conflictos del siglo XXI, razón por la cual se debe tener claridad en sus conceptos, alcances e implicaciones.

La guerra no convencional como dinamizador de la guerra especial

La guerra no convencional es el dinamizador indiscutible de la guerra especial. Esta relación funcional es posible porque las OO. EE. requieren de una innovación constante, en la medida en que las amenazas evolucionan de forma acelerada. Esta velocidad de cambio exige tácticas, técnicas y procedimientos actualizados constantemente con el fin de negarle cualquier tipo de ventaja al enemigo.

La guerra no convencional se ha convertido en una herramienta decisiva a la hora de configurar el campo de batalla. Por supuesto no se limita a esta acción, aunque sería importante responder el siguiente interrogante, aparentemente tautológico: ¿Es la guerra no convencional la respuesta Estatal a los conflictos del siglo XXI?

Y la respuesta es que probablemente sí. Se puede analizar que la capacidad de guerra no convencional ha sido empleada directa o indirectamente en las diferentes generaciones de la guerra. Basta con mencionar, por ejemplo, las operaciones desarrolladas por los Special Air Service (SAS) británicos y la resistencia francesa

durante la Segunda Guerra Mundial, o las misiones que realizaron las FF. EE. estadounidenses en Afganistán tras los ataques del 11 de septiembre.

La guerra no convencional, por tanto, tiene varias características que la convierten en una técnica versátil, lo cual permite emplearla en diferentes ambientes operacionales sin limitarla misionalmente a una situación operacional en particular. Por ello es tan útil en entornos grises, difusos, asimétricos o híbridos. Como se mencionó anteriormente, la doctrina colombiana define la guerra no convencional como aquellas “actividades conducidas en un ambiente de conflicto, orientadas a la búsqueda de inteligencia para debilitar la capacidad de lucha del adversario” (Ejército Nacional de Colombia, 2017b, p. 21). Acá es donde se enlaza con la propuesta mencionada en el primer acápite, de la mano de la Inteligencia y sin ser una tarea exclusiva de ella.

Ahora bien, desde el punto de vista del Ejército de los Estados Unidos –que acerca más fácilmente las FF. EE. a la Inteligencia militar–, la guerra no convencional no se limita a actividades orientadas a la búsqueda de inteligencia, sino que tiene una variedad de acciones, las cuales ayudan exponencialmente a configurar el ambiente operacional facilitando las operaciones militares futuras que se estructuran de acuerdo con la estrategia nacional.

Según el apéndice “A” del *ATP 3-05.1 Unconventional Warfare* del Ejército de los Estados Unidos de América (Department of the Army, 2013), las FF. EE. del Ejército de los Estados Unidos tiene 17 misiones específicas de guerra no convencional, dentro de las cuales se encuentra “localizar y recuperar personal y equipamiento en y desde el área conjunta de operaciones especiales, y garantizar o coordinar el combate conjunto” (s. p.). Como evidencia esta definición, en algunos Estados la guerra no convencional se utiliza para ir más allá de misiones relacionadas con la Inteligencia y, por el contrario, utilizan este tipo de capacidades para desarrollar tareas ofensivas, defensivas y de estabilidad.

En el caso colombiano, si bien existe una estructura doctrinal definida, aún no se han desarrollado todos los Manuales de Campaña del Ejército (MCE), ni tampoco los Manuales de Técnicas del Ejército (MTE), lo cual ha afectado el desarrollo doctrinal de las capacidades críticas de las FF. EE.

El primer paso para construir o fundamentar la guerra no convencional como un dinamizador de la capacidad crítica de guerra especial es definir los manuales de campaña y de técnicas que corresponden al tipo de tareas que realizan las FF. EE. Otra variable muy importante es la voluntad del Comando Superior para el desarrollo creíble de esta capacidad, asumiendo los riesgos estratégicos que esto conllevaría. La guerra no convencional requiere de personal altamente entrenado,

rigurosamente seleccionado, completamente equipado y moralmente fuerte, puesto que esta tarea, a diferencia de las otras, se debe desarrollar de muy bajo perfil y siempre con la autorización y guía del más alto nivel de decisión de una nación.

Tal vez una de las dificultades más importantes en relación con la selección de personal tiene que ver no solo con la comprensión de entornos operacionales ajenos, sino con la cercanía o lejanía del operador especial con patrones culturales diferentes. Un mundo hiperconectado, donde las amenazas transnacionales redundan el carácter difuso de las amenazas híbridas, requiere combatientes con facilidad para operar en leguas extranjeras, conocer e interiorizar patrones culturales diametralmente opuestos a los propios y una capacidad de mimetismo mucho mayor que en cualquier otro momento de la historia, no solo por la hiperconectividad cultural, sino también por el altísimo nivel de exposición mediática y de bases de datos que pueden filtrarse hacia gobiernos, agentes o estructuras adversarias.

El proceso de selección y priorización de blancos también se ofrece como un tema extremadamente sensible en la guerra no convencional. Este proceso requiere caminar un filo muy delgado dada la frontera borrosa del blanco legítimo militar. Se requiere, por tanto, altas e inmejorables capacidades de Inteligencia, de forma que se seleccionen blancos para destrucción, sabotaje o neutralización tras las líneas enemigas, que no impliquen una afectación civil directa, pero que estén dentro del rango de afectación de un adversario que se mueve en zona gris y en dimensiones múltiples.

Con los elementos presentados en este análisis resulta imperioso reconfigurar el concepto doctrinal de la guerra no convencional según la doctrina colombiana. Este no se debe limitar a labores de búsqueda de Inteligencia, sino que, siguiendo el modelo estadounidense, entre otros, se debe poder aplicar en un amplio espectro, de carácter híbrido y entendiendo la multidimensionalidad de las amenazas del presente y el futuro.

Como conclusión preliminar es necesario destacar que las operaciones que se pueden desarrollar dentro del espectro de la guerra no convencional serían una respuesta eficiente, por lo menos en la teoría, ante las amenazas híbridas, las cuales no se pueden combatir con medios convencionales, pues tienen una “combinación diversa y dinámica de fuerzas convencionales, fuerzas irregulares, fuerzas terroristas y/o elementos criminales unificados para lograr efectos mutuamente beneficiosos” (Ejército Nacional de Colombia, 2017c). Quizá la amenaza híbrida requiere de una respuesta híbrida por parte del Estado, escenario en el cual la guerra no convencional es la tarea de la guerra especial que ofrece mayor versatilidad respecto a sus modos, fines y medios para combatir este tipo de amenaza.

La defensa interna en el extranjero como estrategia de seguridad nacional

Dentro del espectro de la guerra especial, la defensa interna en el extranjero se convierte en el complemento ideal para combatir en entornos híbridos.

Para empezar, se debe comprender que la seguridad nacional “es el esfuerzo nacional para prevenir los ataques terroristas, reducir las vulnerabilidades a estos, atender desastres naturales y otras emergencias” (Ejército Nacional de Colombia, 2017c, p. 4-21). Es así como la seguridad nacional se debe considerar como un elemento más de la política de seguridad nacional, en la cual se requiere de una verdadera acción unificada, entendida esta como “la sincronización y/o integración de actividades de entidades gubernamentales y no gubernamentales con las operaciones militares para lograr la unidad de esfuerzo” (Ejército Nacional de Colombia, 2017c, p. 12). Sin esta sincronización es muy difícil desarrollar la estrategia de seguridad nacional, puesto que, como se definió anteriormente, la seguridad es un asunto que compromete no solamente a la fuerza pública, sino también a las autoridades políticas, entre otros actores.

Para los espacios fronterizos, la acción unificada no se debe limitar a las coordinaciones internas, sino que se pueden potencializar, si el caso lo permite, desarrollando coordinaciones con los países amigos. Para ejecutar operaciones militares con otros países se deben dar primero unas condiciones especiales, tales como la estandarización de los procedimientos militares entre los Estados y, por supuesto, la voluntad política para hacerlas. Como se ha mencionado, es necesario recalcar que, debido a la complejidad y a su efecto, el desarrollo y la aplicación de las capacidades críticas y de las operaciones distintivas de las FF. EE. deben contar con la autorización del comandante y jefe de las Fuerzas Militares, quien, en el caso colombiano, es el Presidente de la República, tal y como lo establece la Constitución en su artículo 189: “Dirigir la fuerza pública y disponer de ella como comandante supremo de las Fuerzas Armadas de Colombia” (Constitución Política de Colombia, 1991, art. 189).

Como parte de las capacidades de la guerra especial existe la defensa interna en el extranjero, la cual constituye un multiplicador de la acción unificada del interior en el exterior, o dicho en otras palabras, este tipo de OO. EE. consiste en defender el interior desde el exterior. Este concepto no se debe confundir con otros cercanos como los de *intervención*, *interferencia* u *operaciones de inestabilidad*, los cuales –especialmente el último– son controversiales y con una muy exigua conceptualización. Específicamente, la defensa interna en el extranjero es

la “participación de las agencias civiles y militares de un gobierno, en cualquiera de los programas de acción adoptados por otro gobierno, con el propósito de proteger su sociedad de la subversión, la anarquía, la insurgencia, el terrorismo y otras amenazas” (Ejército Nacional de Colombia, 2018, p. 1-6). Analizando esta definición, se puede concluir que la defensa interna en el extranjero es básicamente una acción unificada coordinada y ejecutada con la participación de organizaciones de otros países que tiene el propósito de proteger el interior de la nación.

El anterior planteamiento hace referencia exclusiva a la doctrina de las FF. EE. del Ejército Nacional de Colombia, de manera que es importante destacar que para otros países la defensa interna en el extranjero no está limitada a unidades de FF. EE., sino que tiene un enfoque global e implica la interacción de esfuerzos multinacionales y operaciones conjuntas entre las fuerzas armadas y las agencias gubernamentales y no gubernamentales. “En general, los esfuerzos del Ejército incluyen a las unidades de Operaciones Especiales, particularmente a los Asuntos Cívico-Militares, Operaciones de Información y Fuerzas Especiales” (Department of the Army, 2015, p. 2-31).

Se debe destacar que, a diferencia de la doctrina colombiana, la doctrina del Ejército de los Estados Unidos incluye las Unidades de Operaciones de Apoyo a la Información Militar (MISO) y las de Asuntos Civiles (CA) dentro de la estructura organizacional de las unidades de OO. EE. En el caso de Colombia, este tipo de unidades no forman parte de la estructura organizacional de las FF. EE. –como unidades, específicamente hablando– (tabla 1).

Tabla 1. *Tareas y subtareas de la defensa interna en el extranjero.*

Defensa Interna en el Extranjero (FID)	Tareas	Subtareas
Participación de las agencias civiles y militares de un gobierno en cualquiera de los programas de acción adoptados por otro gobierno u otra organización designada para liberar y proteger su sociedad de la subversión, la anarquía, la insurgencia, el terrorismo y otras amenazas a su seguridad (MFRE 3-0)	Apoyo indirecto	- Cooperación en seguridad. - Asistencia a fuerzas de seguridad. - Ejercicios conjuntos y/o multinacionales. - Programas de intercambio.
	Apoyo directo sin operaciones de combate	- Asuntos civiles (AC). - Operaciones de apoyo a la información militar. - Apoyo de entrenamiento militar. - Apoyo logístico.
	Apoyo directo con operaciones de combate	- (APQ) Solución temporal decisión presidencial.

Fuente: Ejército Nacional de Colombia (2017c).

El desarrollo de la defensa interna en el extranjero es una pieza clave para la seguridad nacional, pues este tipo de operaciones de las FF. EE. le permiten al Gobierno diseñar una estrategia de seguridad nacional multidimensional. Esta estrategia es ejecutada a través de herramientas militares con capacidades de FF. EE., las cuales, en compañía de las buenas relaciones diplomáticas, en especial con los países limítrofes, pueden crear una acción unificada que esté integrada por todas la capacidades de índole militar y civil de dos naciones aliadas.

En la doctrina de los Estados Unidos, la defensa interna desde el extranjero tiene un enfoque acorde con sus capacidades políticas y militares, así como, evidentemente, con su estatus como potencia. Campañas recientes como las desarrolladas en Afganistán e Irak han ampliado la discusión sobre las formas, métodos, tácticas y técnicas que se emplean en esta herramienta. Así las cosas, se puede plantear que las experiencias compartidas de las Fuerzas de Operaciones Especiales en Irak o Afganistán fueron positivas; sin embargo, el mando conjunto e incluso la misma comandancia de las agrupaciones especiales deben discutir sobre la complejidad de balancear los objetivos a corto plazo y las tareas que busquen alguna solución a largo plazo en la lucha antiterrorista global. En estas soluciones a largo plazo, las FF. EE. ofrecen a los Estados opciones estratégicas y operativas que solo ellas tienen, por medio de reconocimiento especial y acción directa de apoyo a Fuerzas de Tarea Conjunta. Así las cosas, las actividades de defensa interna desde el extranjero son el mejor método para obtener resultados contra estructuras terroristas transnacionales y sus Estados hospederos (Liller, 2005).

Al respecto, el *Manual JP 3-22 Foreign Internal Defense* (FID), que aborda desde una óptica doctrinal el tema, plantea que

[...] si bien la FID es una de las actividades de operaciones especiales centrales designadas del Comando de Operaciones Especiales de los Estados Unidos (USSOCOM) y sus comandos subordinados, la FID puede recibir el apoyo de la Fuerza Conjunta, las Fuerzas Multinacionales (MNF) y otros departamentos y agencias del USG. (Joint Chiefs of Staff [JCS], 2021, p. 14)

Lo relevante es que, en su naturaleza, Estados Unidos no define la defensa interna desde el extranjero como una operación fundamentalmente militar. En lugar de esto, propone que, más bien, normalmente incluye un enfoque interorganizacional

para ayudar a la seguridad, la estabilidad y el desarrollo de un Estado. La defensa interna en el extranjero requiere que todo el gobierno se enfoque en lograr y aprovechar la acción unificada de todos los participantes a través de la facilitación de prácticas como la interoperabilidad, la integración y la interdependencia (JCS, 2021).

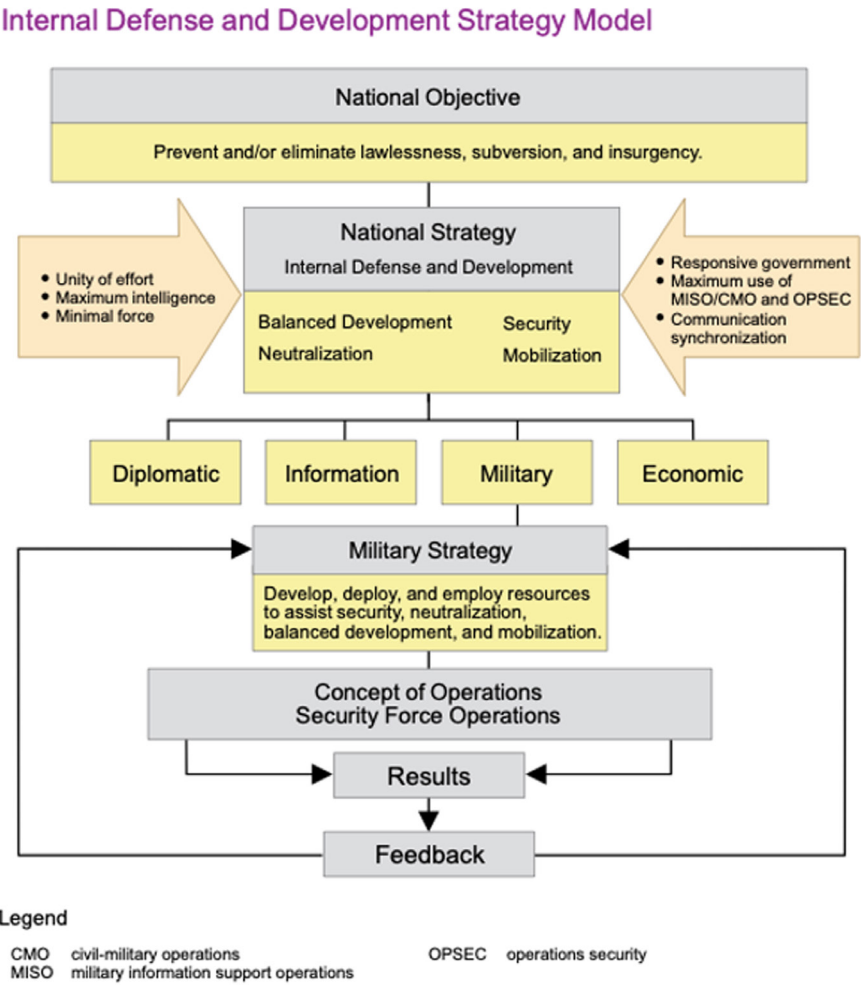
La doctrina estadounidense es enfática en este aspecto, de manera que define unas características de la defensa interna en el extranjero que evidencian la necesidad de tener una visión mucho más amplia de la usual. Específicamente, los Estados Unidos establecen las siguientes características de la defensa interna en el extranjero (JCS, 2021):

- Involucra todos los instrumentos del poder nacional.
- Puede ocurrir en toda la gama de operaciones militares.
- Se lleva a cabo tanto por fuerzas convencionales como por Fuerzas de Operaciones Especiales.
- Apoya e influye en el programa de desarrollo y defensa interna de la nación anfitriona.
- Incluye entrenamiento, material, asistencia técnica y organizativa, asesoría, desarrollo de infraestructura y operaciones tácticas.
- Generalmente, los métodos preferidos de apoyo se realizan mediante programas de asistencia y desarrollo.

Estas características permiten ver dos elementos. El primero, que requiere de todo un esfuerzo concertado e interoperable para llevar a cabo una defensa interna en el extranjero. El segundo, que, desde el Rango de Operaciones Militares (ROM), es una herramienta de complemento a la guerra no convencional en el difícil contexto de la guerra híbrida. Por ello, su aplicación militar no es exclusiva, pero es primordial, desde las FF. EE.

En su ejecución, y tal como aparece en la figura 2, también se ve el carácter estructural de la defensa interna en el extranjero. La doctrina de los Estados Unidos involucra una amplia gama de actores y procesos, de forma que la acción es sostenible y contundente.

Figura 2. Modelo de estrategia de desarrollo y defensa interna en el extranjero.



Fuente: JCS (2021).

No cabe duda de que, por su condición, la concepción que tienen los Estados Unidos de la defensa interna en el extranjero es diferente de la colombiana. Aún así, es posible establecer paralelos en cuanto a la complementariedad desde lo militar con la guerra no convencional, pero también con la necesidad de entenderla como una herramienta que debe involucrar a la mayor parte de agencias, de forma que el alcance sea más amplio y su efecto sea concertado.

En conclusión, la defensa interna en el extranjero le permite a Colombia, a través de las FF. EE., proyectar capacidades militares en pro de fortalecer y garantizar

la seguridad nacional, así como fortalecer las relaciones internacionales con los países aliados, con quienes eventualmente se desarrollarían este tipo de operaciones. Es precisamente por la anterior característica que la defensa interna en el extranjero se diferencia de las otras clases de operaciones que involucran la capacidad crítica de guerra especial: la participación directa o indirecta de otro país en una visión holística de seguridad, entendiendo que si se garantiza la seguridad regional, se fortalece la seguridad nacional.

Conclusiones

En entornos extremadamente cambiantes y dinámicos como las guerras híbridas, se requieren componentes militares igualmente cambiantes, dinámicos, adaptativos y flexibles. Es por ello que las FF. EE. se convierten en la herramienta de mayor valor estratégico en estos teatros operacionales.

Más allá de las capacidades de ataques de precisión quirúrgica, es en la guerra especial como se encuentran las respuestas a los retos híbridos. Ahora bien, aunque la guerra no convencional y la defensa interna en el extranjero son dos tareas complementarias dentro de la guerra especial, estas deben ser revisadas tanto en sus definiciones como en sus planteamientos para poder articularlas y llevarlas a fondo.

En primer lugar, se requiere una unidad de esfuerzo que sea el producto de una acción unificada exitosa, que es esencial para prevenir crisis y derrotar amenazas creíbles. En segundo lugar, la construcción de una nueva Inteligencia es fundamental, de tal forma que su uso optimizado requiere que todas las operaciones se basen en inteligencia confiable, precisa, relevante y oportuna, pero que también esté fusionada con las FF. EE. en tiempo, modo y lugar.

En tercer lugar, se requiere un uso sincronizado de las Operaciones de Apoyo de Información Militar (MISO, por la sigla en inglés de Military Information Support Operations) con otras actividades operativas, pues esto puede mejorar la legitimidad de las FF. EE. involucradas en la acción.

Por último, se debe generar una sinergia no solo con el conductor político, sino también con el mando estratégico y operacional. Esta organización debe proporcionar planificación y dirección centralizadas, facilitar la ejecución descentralizada del plan y estar estructurada y autorizada para que pueda coordinar y dirigir los esfuerzos de la guerra no convencional y la defensa interna en el extranjero. Así las cosas, el reto doctrinal en Colombia está abierto y la necesidad de llevar la doctrina más allá es evidente.

Referencias

- Álvarez Calderón, C. E. (Ed.). (2017). *Escenarios y desafíos de la seguridad multidimensional en Colombia*. Sello Editorial ESDEG. <https://doi.org/10.25062/9789585652835>
- Colom, G. (2012). Vigencia y limitaciones de la guerra híbrida. *Revista Científica General José María Córdova*, 10(10), 77-90. <https://doi.org/10.21830/19006586.228>
- Colom, G. (2018). Guerras híbridas: Cuando el contexto lo es todo. *Revista Ejército*, (927), 38-44. <https://tinyurl.com/4tk6b55d>
- Department of the Army. (2010). *Training Circular TC 18-01 Special Forces Unconventional Warfare*. Department of the Army. <https://tinyurl.com/49ez2xf4>
- Department of the Army. (2013). *Army Techniques Publication ATP 3-05.1 Unconventional Warfare*. Department of the Army.
- Department of the Army. (2014). *Field Manual FM 3-18 Special Forces Operations*. Department of the Army. <https://tinyurl.com/yn6h6atz>
- Department of the Army. (2015). *Army Techniques Publication ATP 3-05.2 Foreign Internal Defense*. Department of the Army. <https://tinyurl.com/ym23fyjx>
- Ejército de Chile. (2013). *Memorial del Ejército de Chile*. Departamento Comunicacional del Ejército. <https://tinyurl.com/5d7nsukd>
- Ejército Nacional de Colombia. (2017a). *Manual Fundamental del Ejército MFE 3-05 Operaciones Especiales [Público]*. Imprenta Militar del Ejército. <https://tinyurl.com/2p8b7nse>
- Ejército Nacional de Colombia. (2017b). *Manual Fundamental del Ejército MFE 3-05 Operaciones Especiales [Público]*. Imprenta Militar del Ejército. <https://tinyurl.com/2p8b7nse>
- Ejército Nacional de Colombia. (2017c). *Manual Fundamental de Referencia del Ejército MFRE 3-0 Operaciones [Público]*. Imprenta Ejército. <https://tinyurl.com/ducmt7je>
- Ejército Nacional de Colombia. (2018). *Manual de Campaña del Ejército MCE 3-18 Operaciones de Fuerzas Especiales [Restringido]*. Imprenta Ejército.
- Equilibrium Global. (2020, 21 de noviembre). Entendiendo la guerra híbrida en la práctica. <https://tinyurl.com/yjbzx836>
- González, M. A., & Betancourt, M. A. (2018). La transformación del Ejército Nacional de Colombia: Una interpretación teórica. *Revista Latinoamericana de Estudios de Seguridad*, (22), 70-84. <http://dx.doi.org/10.17141/urvio.22.2018.3093>
- Joint Chiefs of Staff [JCS]. (2021). *Foreign Internal Defense* [Joint Publication, N.º 3-22]. JCS. <https://tinyurl.com/bdf5bj8>
- Linnemann, R. A. (2016). El arte no convencional y la guerra moderna. *Military Review*, (julio-septiembre), 30-39. <https://tinyurl.com/3xwx5nby>
- Liller, O. K. (2005). *Special Operations Forces and Foreign Internal Defense: An effective counterterrorism method* [Trabajo de grado, Naval War College]. Repositorio DTIC. <https://tinyurl.com/44tuxjax>

- Montero, L. A. (2022, 7 de marzo). Guerras híbridas: La naturaleza cambiante de la guerra [Video]. YouTube. https://www.youtube.com/watch?v=ZNYiBeEla_I&t=32s
- Montero, L. A., Niño, J. A., Ríos, J. A., Orduz, A. L., & Yasno, J. A. (2020). El oso vuelve al combate: El tridente estratégico para operaciones encubiertas e híbridas en Rusia. En M. A. González-Martínez & L. A. Montero-Moncada (Eds.), *El tridente del poder estratégico: Inteligencia, Operaciones Especiales y poder ciber en el siglo XXI* (pp. 43-62). Sello Editorial ESDEG. <https://doi.org/10.25062/9789584288943.02>
- Rodríguez-Álvarez, F., & Montero-Moncada, A. (2022). Operaciones de interferencia en ciberseguridad y ciberdefensa: Herramienta estratégica para la supervivencia de los Estados. En L. A. Montero-Moncada (Ed.), *Poder y estrategia: Elementos para la supervivencia del Estado* (pp. 227-301). Sello Editorial ESDEG. <https://doi.org/10.25062/9786289530483.09>
- Rojas Guevara, P. J. (2017). Doctrina Damasco: Eje articulador de la segunda gran reforma del Ejército Nacional de Colombia. *Revista Científica General José María Córdova*, 15(19), 95-119. <https://doi.org/10.21830/19006586.78>

Capítulo 7

Soporte ciber a Fuerzas Especiales del Ejército colombiano en ambiente táctico*

DOI: <https://doi.org/10.25062/9786287602809.07>

Juan Guillermo Cruz Segura

Ricardo Di Genaro

Escuela Superior de Guerra "General Rafael Reyes Prieto"

Resumen: Las operaciones ciber ofrecen a los gobiernos una capacidad más en su búsqueda de afectar al adversario sin usar la violencia con armas convencionales. Las guerras de quinta generación son el escenario propicio para desarrollar estas operaciones. El objetivo del capítulo es identificar cómo las Fuerzas Especiales del Ejército Nacional podrían emplear estas capacidades para cumplir objetivos tácticos y estratégicos, teniendo en cuenta que este tipo de unidades especiales son el bastión estratégico de las Fuerzas Militares del país y sus objetivos son de alto valor estratégico. Se emplea la doctrina actual de las Fuerzas Militares de Colombia y del Ejército Nacional en conjunto para abordar este tema, que, junto a algunos casos tácticos mundiales, permiten identificar la importancia y alcance de este tipo de operaciones.

Palabras clave: Fuerzas Especiales; guerras de quinta generación; guerra híbrida; hardware; operaciones ciber; operaciones especiales; software.

* Este capítulo es resultado de investigación adscrito al proyecto "Naturaleza de la guerra contemporánea. Retos y oportunidades de las Fuerzas Especiales y la Inteligencia", adscrito al Departamento Ejército de la Escuela Superior de Guerra, inscrito en la línea de investigación "Naturaleza de la guerra, terrorismo, nuevas amenazas", que forma parte del grupo de investigación Centro de Gravedad, categorizado en A por Minciencias, con código COL0104976. Los puntos de vista pertenecen a los autores y no reflejan necesariamente los de las instituciones participantes.

Juan Guillermo Cruz Segura

Teniente Coronel del Ejército Nacional de Colombia. Maestrando en Estrategia y Geopolítica, Escuela Superior de Guerra "General Rafael Reyes Prieto", Colombia. Especialista en Conducción y Administración de Unidades Militares, y especialista en Administración de Recursos Militares para la Defensa Nacional, Escuela de Armas y Servicios. Profesional en Ciencias Militares, Escuela Militar de Cadetes "General José María Córdova", Colombia. Contacto: juan.cruzse@buzonejercito.mil.co

Ricardo Di Genaro

Mayor del Ejército Argentino. Maestrando en Relaciones Internacionales, Universidad de Belgrano. Especialista en Conducción de Organizaciones Militares Terrestres, Escuela Superior de Guerra "General Luis María Campos", Argentina. Diplomado en Inteligencia Económica para la Defensa, Universidad Bernardo O'Higgins, Chile. Diplomado en Docencia Universitaria y Herramientas Pedagógicas de Aprendizaje, Escuela Naval de Cadetes "Almirante Padilla", Colombia. Licenciado en Administración, Colegio Militar de la Nación, Argentina. Contacto: rdigenaro@ejercito.mil.ar

Citación APA: Cruz Segura, J. G., & Di Genaro, R. (2024). Soporte ciber a Fuerzas Especiales del Ejército colombiano en ambiente táctico. En L. Montero Moncada & O. A. Garzón Gómez (Eds.), *Comandos: Retos de las Fuerzas Especiales e Inteligencia en la guerra contemporánea* (pp. 163-188). Sello Editorial ESDEG.
<https://doi.org/10.25062/9786287602809.07>

COMANDOS: RETOS DE LAS FUERZAS ESPECIALES E INTELIGENCIA EN LA GUERRA CONTEMPORÁNEA

ISBN impreso: 978-628-7602-79-3

ISBN digital: 978-628-7602-80-9

DOI: <https://doi.org/10.25062/9786287602809>

Colección Seguridad y Defensa

Sello Editorial ESDEG

Escuela Superior de Guerra "General Rafael Reyes Prieto"

Bogotá D.C., Colombia

2024



Introducción

De acuerdo con el Centro de Doctrina del Ejército Nacional (CEDOC), la doctrina es el conjunto de principios fundamentales, con sus correspondientes tácticas, técnicas, procedimientos, términos y símbolos, que, empleados en conjunto, permiten la conducción de las operaciones. Mediante estos principios, el Ejército de combate y los elementos del Ejército generador de fuerza –que apoyan directamente las operaciones– guían sus acciones en cumplimiento de los objetivos nacionales. Además, la doctrina se puede entender como una guía sobre cómo (no qué) pensar, preparar y ejecutar partes esenciales del proceso de operaciones y entrenamientos. En consecuencia, se puede afirmar que la doctrina se adapta a las circunstancias particulares del momento de su aplicación y en muy pocas ocasiones es impositiva (Salazar, 2020).

No obstante esta claridad conceptual, las Fuerzas Especiales (FF. EE.) del Ejército Nacional de Colombia no cuentan con una base doctrinal específica para emplear sus capacidades en las operaciones ciber en un ambiente táctico. Si se sube de nivel, se encuentra que el Estado Mayor del Comando del Ejército establece la doctrina sobre operaciones en la organización, específicamente en el *Manual de Campaña del Ejército MCE 3-12, Operaciones del Ciber Espacio*, un documento de carácter restringido. Además, un escalón más arriba, en el Comando General de las Fuerzas Militares (CGFM) existe actualmente un Comando Conjunto de Operaciones Cibernéticas, que tiene la misión de planear, coordinar, integrar y conducir operaciones militares en el ciberespacio para defender los intereses nacionales y la infraestructura crítica cibernética nacional, a fin de contribuir en el cumplimiento de la misión del CGFM (Comando Conjunto Cibernético [CCOCI], 2020).

Cabe señalar que un comando conjunto se entiende como un “comando unificado o específico con una misión amplia y continua, designado desde el nivel

estratégico” (CGFM, 2018, s. p.). En este sentido, los principales roles y funciones del Comando Conjunto de Operaciones Cibernéticas son asesorar al Presidente de la República, al Ministro de Defensa y al Consejo Superior de la Defensa Nacional en asuntos militares, así como preparar y definir planes para desarrollar políticas de seguridad nacional, entre muchas otras.

A pesar de lo anterior, la falta de información y de doctrina en las FF. EE. evidencia los vacíos de conocimientos que hay en la institución. Cuando se baja de nivel, esta falencia hace que se pierda una capacidad que se podría emplear con las FF. EE. y sus roles dentro del ambiente táctico. Precisamente, el objetivo del capítulo es aportar insumos que contribuyan a que las unidades de FF. EE. desarrollen la capacidad de soporte ciber o que la empleen como un apoyo directo en la misión. Con este propósito, se hace un análisis prospectivo de las oportunidades, ventajas y falencias que se podrían generar en este tipo de capacidades militares, con el entendido de que esta combinación tiene una gran incidencia en el espectro de la guerra híbrida que vive a diario Colombia, en la cual existen diversidad de fenómenos criminales y de inestabilidad que afectan el orden público.

En este sentido, analizar la doctrina existente constituye un aporte al incipiente estado de la literatura académica, que poco se ha ocupado de este tema. Así, este capítulo contribuye a los esfuerzos institucionales para continuar con la investigación metódica sobre Doctrina, Organización, Material y Equipo, Personal, Infraestructura, Liderazgo, Educación (entrenamiento incluido) y Mantenimiento (DOMPILEM) (Ejército Nacional de Colombia, 2017), para medir el estado actual de algún tipo de capacidad o unidad militar.

Como se mencionó, las investigaciones académicas no han estudiado la manera en que las unidades de Operaciones Especiales (OO. EE.) del Ejército de Colombia, destacadas en el Comando Conjunto de Operaciones Especiales –rectora de la doctrina y empleo de este tipo de unidades–, pueden emplear la capacidad ciber, sea como apoyo directo a las operaciones o como unidades orgánicas dentro de las especialidades de las FF. EE., en el ambiente táctico. Este último se entiende como la acción táctica, las batallas, los encuentros o los combates que emplean acciones letales y no letales diseñadas para un propósito específico en relación con el enemigo, el terreno, las fuerzas amigas u otras entidades (Ejército Nacional de Colombia, 2017b).

Por esta razón, en este trabajo se abordan temas que no están descritos en la doctrina de las FF. EE. del Ejército Nacional con el propósito de apoyar las teorías, técnicas y tácticas que requiere esta unidad para ejecutar operaciones

cibernéticas en función de la consecución de los objetivos estratégicos de la nación. Específicamente, se busca suplir vacíos como los alcances operacionales y tácticos de las operaciones ciber en el nivel táctico de las FF. EE., sus debilidades y cuál puede ser la proyección del empleo y organización de esta nueva especialidad en las unidades especiales y, más importante aún, cómo aplicarlas en el ámbito de la guerra híbrida en Colombia.

Relación doctrinal

A través de la historia, la humanidad se ha visto envuelta en varios acontecimientos en que dos o más partes buscan imponer su voluntad por medio de la fuerza física o la violencia; esta es, precisamente, una definición general del concepto de guerra. Con el paso de los años, esta acepción se ha mantenido, pero la guerra en su naturaleza ha evolucionado de diferentes formas. En la actualidad hablamos de guerra híbrida, término acuñado en 2007 por Frank Hoffman (2007)¹ para aludir a la conjunción de modos y estrategias de guerra militares convencionales, enlazándolos con tácticas terroristas que abarcaban la violencia y el desorden criminal (Azabal, 2021).

Dentro de este tipo de guerras, en las cuales se combate en diferentes frentes, se encuentran las guerras cibernéticas. En los últimos años, uno de los espectros en donde han tomado fuerza las tecnologías y el desarrollo de las TIC, tanto en el ámbito civil como en el militar, es el ciberespacio, entendido como el entorno no físico creado por equipos de cómputo unidos para interoperar en una red (EcuRed, 2012).

Este mundo virtual se ha convertido en una de las fortalezas, ventajas o capacidades de las fuerzas armadas en el mundo. En este contexto, las Fuerzas Militares de Colombia se han ajustado a los retos que conlleva la globalización y la actualización de tecnologías, de manera que han creado doctrina y organizaciones que poseen las capacidades necesarias para defender a la nación en este escenario, como las operaciones ofensivas o de ataques para neutralizar cualquier intención hostil.

Otro concepto del ámbito de la cibernética muy llamativo es el de ciberguerra, que se puede entender como una agresión promovida por un Estado contra otro con la intención de cumplir algún objetivo estratégico. En esencia, la ciberguerra

¹ Teniente coronel del Ejército de los Estados Unidos de América, en la reserva, que se desempeña como investigador en la Universidad Nacional de Defensa (Departamento de Defensa).

busca dañar gravemente las capacidades del oponente para imponerle la aceptación de un objetivo propio o, simplemente, para sustraerle o robarle información esencial que pueda usar posteriormente, cortar o destruir sus sistemas de comunicación o alterar sus bases de datos.

En otras palabras, el concepto abarca lo que habitualmente se ha entendido como guerra, pero con la diferencia de que el medio empleado no sería la violencia física, sino un ataque informático (a través de sistemas y redes) que permita obtener una ventaja sobre el enemigo para situarse en superioridad, o incluso para derrocarlo (Sánchez, 2009). En un escenario de ciberguerra se realizan diversas operaciones, entre las cuales se encuentran: la explotación, entendida como la obtención de información de los destinatarios; el engaño, en donde se manipula la información recolectada; la destrucción, que busca hacer inoperable el objetivo, y, por último, la interrupción, en la cual no se destruye el objetivo, pero se deja inoperante.

No se puede hablar de ciberguerra sin entender el concepto de ciberterrorismo. Este término se refiere a la convergencia del ciberespacio y el terrorismo, es decir, la forma en la que el terrorismo utiliza y emplea las tecnologías de la información, que están en constante evolución, para intimidar, coaccionar o para causar daños a grupos sociales específicos con fines políticos-religiosos. Por tanto, el ciberterrorismo es una nueva forma de combatir en la que el terrorismo cambia las armas, las bombas y los misiles por una computadora y demás elementos informáticos para planificar y ejecutar ataques ofensivos y defensivos que produzcan los mayores daños posibles a la población civil (Sánchez, 2009).

Por su parte, las operaciones de información se entienden como las actividades relacionadas con el empleo integrado de las capacidades de guerra electrónica, operaciones de redes informáticas, operaciones de apoyo a la información militar, engaño militar y operaciones de seguridad, para generar condiciones de éxito y prevalecer en el ambiente de información militar (Ejército Nacional de Colombia, 2017a). Estas forman parte de la gran cadena de posibilidades de operaciones que pueden apoyar las FF. EE. en el espectro del ciberespacio. Específicamente, en la doctrina colombiana se indica que las operaciones de información son todas las actividades de tipo electrónico que podrían apoyar una batalla.

Las operaciones de información tienen el propósito de afectar el ciclo de toma de decisiones de los líderes del adversario y proteger el propio, por medio de acciones desarrolladas y encaminadas en diferentes dominios. Las operaciones que son ejecutadas en el dominio físico buscan atacar o defender la infraestructura física asociada al mando y el control, así como a la toma de decisiones de los

comandantes en todos los niveles. En este escenario los objetivos típicos son las redes de comunicaciones, los sensores, los medios de búsqueda y los propios mandos, entre otros aspectos que son susceptibles de ser afectados por medios kinésicos tradicionales (que emplean movimiento por fuego).

En el dominio cognitivo o de conocimiento, se ejecutan operaciones destinadas a afectar la percepción por parte de los tomadores de decisiones en los diferentes campos de acción de batalla. En este caso, el instrumento típico para realizar las operaciones psicológicas son el engaño o la decepción militar, aunque también pueden considerarse como parte de estas (Ejército Nacional de Colombia, 2021). Lo que se busca con este tipo de ataques es generar un caos en la toma de decisiones de los líderes en los diferentes niveles para que las precisiones de la táctica y la estrategia fallen en la búsqueda de sus objetivos.

Al hablar de operaciones ciber no se puede dejar de lado el concepto o término de operaciones de quinta generación, también denominada *guerra sin límites*. Definida e introducida desde el 2009 como concepto estratégico operacional en las intervenciones de los Estados Unidos y la Organización del Tratado del Atlántico Norte (OTAN), la guerra de quinta generación determina que no interesa ganar o perder, sino demoler o destruir la fuerza intelectual del enemigo, obligándolo a buscar un compromiso, valiéndose de cualquier medio, incluso sin uso de las armas convencionales. Es decir, se trata de manipular directamente la percepción del ser humano atacando su cerebro, en concreto, su parte neurológica: ondas binaurales y componentes de cristales de magnetita del cerebro y los métodos sobre sus posibles manipulaciones (Aharonian, 2018). En el contexto actual, caracterizado por la gran influencia que tienen las redes sociales y los medios de comunicación sobre las decisiones y los caminos que transita un Estado, estas acciones son una herramienta importante tanto para la defensa como para la ofensiva, de manera que es fundamental tener muy clara esta noción.

Como se puede inferir, la tecnología, entendida como el conjunto de instrumentos y procedimientos industriales de un determinado sector o producto (Real Academia Española, 2022), tiene un papel importante en las guerras de quinta generación. Específicamente, en este estudio la tecnología hace referencia a elementos como computadores, conexiones, redes, software y hardware, entre otros, que emplea una fuerza militar para la defensa de su información, evitando así conflictos en la toma de decisiones cruciales para el desarrollo de las operaciones militares.

Una palabra clave dentro de la tendencia actual de la tecnología y las guerras cibernéticas es el internet. Se trata de un concepto acuñado en los años 80 que fue

definido como “una red de redes de ordenadores capaces de comunicarse entre ellos. No es otra cosa. Sin embargo, esa tecnología es mucho más que una tecnología. Es un medio de comunicación, de interacción y de organización social” (Castells, 2000, p. 9). Actualmente, el internet es la clave para la interconexión de la información a través de la distancia en tiempo real, lo que permite la fluidez de los datos en diversos campos a la vez.

Evidentemente, las organizaciones militares no pueden dejar de lado este concepto, ya que una de las funciones de la conducción de la guerra esenciales para el direccionamiento de la estrategia y la táctica es el mando y control, en el cual, a través de las comunicaciones y sus medios, incluyendo el internet, se puede comunicar la intención del comandante y el objetivo militar que se espera cumplir. Es por esta razón que es vital contar con una ciberdefensa en este campo de acción para evitar ataques que puedan comprometer la seguridad y la soberanía nacionales. Así sucedió el 11 de julio del 2021, cuando los medios de comunicación colombianos revelaron detalles del hackeo más grande contra las Fuerzas Militares de Colombia por parte del gobierno venezolano. La investigación periodística señaló que la inteligencia de ese país, desde seis puntos diferentes del territorio venezolano, había atacado deliberadamente durante meses los servidores del CGFM en Bogotá (Redacción BLU Radio, 2021).

Otro aspecto importante que se debe tener en cuenta son las famosas redes sociales. Sin lugar a duda, una de las grandes revoluciones sociales y tecnológicas como consecuencia del empleo masivo del internet son las redes que conectan a la población de todo el globo terráqueo. La forma de relacionarse con los demás ha pasado de lo personal a la computadora. Las redes sociales actúan como puntos digitales de encuentro donde es posible acceder a información de todo tipo, compartir impresiones, consultar archivos y recursos disponibles en tiempo real, con una velocidad nunca imaginada, como es el caso de Facebook, Hi5, Twitter (ahora X), My Space, etc. Pero aún más útil que tan solo el intercambio de fotos, videos o mensajes, es la creación de otra clase de redes sociales, aquellas que tienen como fin el apoyo y la difusión de diversos temas (Ledo, 2011).

Un ejemplo de esto fue lo ocurrido en las elecciones de los Estados Unidos de 2016, donde resultó electo Donald Trump. En esa oportunidad, la Federación de Rusia ejerció una influencia mediática a través de las redes sociales para que su candidato de preferencia llegara a la Casa Blanca, lo cual les permitiría continuar con sus objetivos estratégicos. El diario *La Vanguardia* señaló que esta campaña rusa dirigió sus esfuerzos hacia usuarios afroamericanos, como parte de sus

tácticas para favorecer el voto del candidato republicano, el presidente de esa época, Donald Trump. Estas son algunas de las conclusiones a las que ha llegado un informe minucioso que fue elaborado para el Comité de Inteligencia del Senado, a cuyo borrador tuvo acceso *The New York Times* (*La Vanguardia*, 2018)

Finalmente, otro aspecto clave es el humano. Como lo ha demostrado la historia militar a lo largo de las distintas generaciones de la guerra, el combatiente es uno de los factores de éxito en su desarrollo. Toda fuerza militar que cuente en sus filas con personal idóneo para planificar, conducir y ejecutar operaciones militares facilitará que se cumplan los objetivos. Por su puesto, este también es el caso de las operaciones ciber, pues contar con personal militar especialista en seguridad cibernética es relevante, ya que estos profesionales controlan, analizan, detectan y responden a la actividad no autorizada en el dominio espacial (*Today's Military*, 2022).

Sin embargo, es importante que el personal que integra los estados mayores del nivel operacional y los comandantes, quienes son finalmente los que toman las decisiones, también tengan conocimientos sobre las operaciones cibernéticas, ya que durante el planeamiento y el desarrollo de la campaña se deberán tomar medidas tanto defensivas, para preservar los propios sistemas, como ofensivas, para afectar los sistemas de la infraestructura crítica y los sistemas de armas enemigos mediante el empleo de armas ciber.

En este sentido, también es importante destacar que el personal responsable de insertar físicamente un dispositivo para infectar una red cerrada de un sistema enemigo debe contar con una rigurosa capacitación. Por ejemplo, durante el año 2010 se empleó el gusano informático Stuxnet, un “misil ciberespacial” de origen desconocido, para sabotear instalaciones nucleares iraníes. Este virus afectó las centrífugas de refinación de combustible nuclear, con lo cual dificultó el desarrollo de uranio de calidad militar. Cabe señalar que el programa nuclear iraní es un sistema cerrado, de manera que la operación debió tener un acceso privilegiado para obtener el conocimiento de sus sistemas informáticos. En ese sentido, se puede apreciar cómo el factor humano fue un aspecto clave para obtener la información que permitiera desarrollar el gusano informático.

Es decir, a diferencia de otros virus que pueden navegar a través de varias redes hasta su blanco, el Stuxnet infectó a su blanco a través de un dispositivo extraíble que fue insertado por un individuo de manera accidental o intencional, pues la única manera de acceder a la red nuclear iraní era por medio del acceso físico a las computadoras que la integran (Fink, 2014).

En conclusión, en el campo de combate moderno es necesario disponer de personal militar idóneo que tenga la capacidad de infiltrarse físicamente en la

infraestructura crítica enemiga, de manera que pueda obtener información de redes informáticas cerradas enemigas o insertar físicamente programas informáticos como un “misil ciberespacial” para poder infligir daños en sus redes, afectar su ciberespacio y, finalmente, causarle daños materiales.

En el caso específico que nos ocupa, habría que enfatizar que las FF. EE. deben poseer personal idóneo en materia de cibernética para estar en la capacidad de servir a las operaciones ciber que ejecute el comando del cual dependen. Asimismo, debe nutrirse del apoyo a las operaciones ciber para que adquiera la capacidad de realizar sus operaciones específicas, como podría ser, por ejemplo, neutralizar el sistema de seguridad de una instalación militar para infiltrarse y sabotearla.

Caracterización de las operaciones ciber

Como se mencionaba en el apartado anterior, el último dominio empleado en las guerras actuales y futuras, denominado el quinto dominio, es el ciberespacial. Específicamente, el ciberespacio es un dominio global dentro del ambiente de la información que consiste en redes interdependientes de infraestructura de tecnologías de la información y datos contenidos, los cuales incluyen: internet, telecomunicaciones, redes, sistemas informáticos y procesadores y controladores integrados (Ejército Nacional de Colombia, 2021).

En el actual desarrollo evolutivo acelerado de la tecnología, cobra vital importancia el control de este dominio global, dada la importancia que reviste para cualquier nación. Objetivos estratégicos nacionales como la información, las finanzas, los sistemas de transporte, las fuerzas militares, la inteligencia estratégica, la salud, la educación, la economía, entre otros, desarrollan todas sus actividades en ambientes virtuales, los cuales son propicios para que el enemigo, conocedor del tema ciberespacial, pueda afectar los procedimientos en cada uno de estos ejes estratégicos y poner en jaque a la nación. Es por esto que el tema de estudio es de carácter prioritario para el Gobierno Nacional y para los estamentos encargados de la defensa y la seguridad del Estado colombiano.

En este contexto, el análisis de las variables operacionales por parte de los expertos en ciberseguridad requiere un estudio a fondo de estos elementos: el ambiente político en el cual se establecen las redes y los nodos que requieren mayor énfasis para el funcionamiento de la Fuerza; el ambiente económico, es decir, qué redes y nodos se requieren para permitir el comercio y la economía de la nación; el ambiente militar, dónde están ubicados los nodos y las redes con las que actúa el

enemigo; el ambiente social, en el cual se analizan las redes de comunicación que tiene la población del país para proporcionar información y protegerlos de efectos negativos; el ambiente de información, donde se verifica cuál es la naturaleza de la información en tránsito que afecta las operaciones militares; el ambiente del tiempo, donde se determina los momentos óptimos que respalden las operaciones; el ambiente de infraestructura, que busca entender qué redes y nodos permiten el funcionamiento de la infraestructura crítica, las capacidades claves de los recursos y el control de los datos; y, por último, el medioambiente físico, en el cual se busca analizar cómo se ven afectadas las redes inalámbricas por los efectos del clima y el terreno (Ejército Nacional de Colombia, 2017b).

El estudio analítico de un estado mayor especializado en el ambiente ciberespacial permite a los comandantes operacionales la mejor toma de decisiones cuando es requerida una intervención, sea en defensa o en acción ofensiva, en el quinto dominio. Además de esto, analizar las variables de la misión (METT-TC): misión, enemigo, tiempo, terreno, tropas disponibles y consideraciones civiles, con énfasis en las tropas disponibles, permite definir el tipo de unidades requeridas; precisamente el tema que se trata en este capítulo.

Para entender mejor la caracterización de las operaciones ciber, es importante comprender qué son y cuáles son las operaciones cibernéticas de Colombia. Específicamente, las operaciones cibernéticas son el conjunto de operaciones militares que se desarrollan en o a través del ciberespacio, es decir, aquellas que se planean y ejecutan con y a través del empleo de recursos cibernéticos, con el propósito de garantizar la seguridad y defensa de la nación y reducir o neutralizar la acción del poder del enemigo para asegurar la ventaja operacional y la adecuada acción del poder militar propio (CGFM, 2016).

Las operaciones de ciberseguridad contribuyen sustancialmente a proteger y asegurar el funcionamiento de la infraestructura crítica cibernética del poder militar y la infraestructura crítica nacional. Dentro de esta infraestructura crítica se pueden encontrar trece sectores: 1) el Gobierno; 2) la seguridad y la defensa; 3) las tecnologías de la información y las comunicaciones; 4) la electricidad; 5) las finanzas; 6) la educación; 7) los recursos minero-energéticos; 8) la industria, el comercio y el turismo; 9) el ambiente; 10) la salud y la protección social; 11) el agua; 12) el transporte y, por último, 13) la alimentación-agricultura.

Las infraestructuras críticas de un Estado son todos aquellos sistemas físicos o virtuales que facilitan funciones y servicios esenciales para apoyar a los sistemas más básicos a nivel social, económico, medioambiental, militar y político. Una

afectación o debilitamiento o ralentización en su funcionamiento debido a causas naturales (por ejemplo: una inundación que afecta al suministro eléctrico) o provocada por el hombre (por ejemplo: un atentado terrorista o un ataque cibernético a una central nuclear o a una entidad financiera) podría ocasionar graves consecuencias a largo y corto plazo (Instituto de Seguridad y Bienestar Laboral, 2023).

Por esta razón, para cualquier Estado es de vital importancia tener un aparato militar especializado, actualizado y entrenado en todos los tipos de operaciones cibernéticas. Las diversas amenazas externas e internas, de índole legal e ilegal, que aparecen en el sistema internacional actual luego de los atentados del 11 de septiembre del 2001 en los Estados Unidos –los cuales cambiaron la forma como se veían las guerras– hacen prioritaria la atención a este tipo de guerras.

Entre las operaciones de ciberseguridad se encuentran las operaciones defensivas, que buscan proteger y asegurar la capacidad de adaptación a situaciones adversas del componente cibernético. A su vez, estas están conformadas por operaciones de prevención, operaciones de análisis y, por último, operaciones de aseguramiento (CGFM, 2016), las cuales, como se verá en el estudio de caso, tienen el objetivo de evitar los ataques cibernéticos por medio de campañas, capacitaciones, análisis, planificación y vigilancia de los sistemas.

Otro tipo de operaciones que forman parte de la ciberseguridad son las operaciones de gestión de incidentes cibernéticos, cuyo objetivo principal es recuperar el nivel de funcionamiento de los sistemas cibernéticos y minimizar los impactos negativos luego de un ataque cibernético. Con estas operaciones se intenta normalizar en tiempo y lugar el funcionamiento de los servicios básicos prestados a la sociedad.

El tercer y último tipo de operación de ciberseguridad es la de protección a la infraestructura crítica cibernética. Con este tipo de operaciones se busca preservar el nivel de normalidad en el funcionamiento de la infraestructura crítica cibernética, de tal manera que pueda continuar la prestación de servicios esenciales a la población y garantizar la gobernabilidad del país (CGFM, 2016).

Para concluir el tema de las operaciones de ciberseguridad, a continuación se aborda otro tipo de operación que también recurre a la cibernética. Puntualmente, las operaciones de ciberdefensa son acciones del tipo no pasivas, es decir, están encaminadas a prevenir, detectar y contrarrestar las amenazas que pongan en riesgo el funcionamiento de las Fuerzas Militares y el orden nacional. Dentro de esta clase se encuentran las operaciones ofensivas, que son aquellas cuyo objeto final es interrumpir, alterar, degradar, engañar y/o destruir sistemas de cómputo,

información, redes, programas, entre otros, con el propósito de afectar el normal funcionamiento y desarrollo de las operaciones del enemigo, causando efectos directos e indirectos en el campo de batalla (CGFM, 2016).

Un claro ejemplo de este tipo de operaciones es el reciente conflicto entre Rusia y Ucrania, en donde hackers rusos usaron un video falso del presidente de Ucrania, Volodimir Zelenski, donde daba órdenes a sus tropas y a sus connacionales instigando a sus compatriotas a que se rindieran. Este video falso apareció en el tabloide ucraniano de lengua rusa *Segodnya*, el cual acusó a hackers enemigos de crear y publicar el *deepfake* en su web. A su vez, el propio Zelenski también desmintió en otro video donde pide a los rusos que sean ellos los que depongan las armas (Kardoudi, 2022). Este ataque cibernético podría haber llevado los destinos de esta guerra por otro rumbo si las fuerzas cibernéticas no se hubieran dado cuenta a tiempo de la situación crítica que el video podría propiciar.

Dentro de este tipo de operaciones se pueden desarrollar actividades como la infiltración, la infección, la denegación del servicio de cibernética, las actividades contra la seguridad de los datos, la degradación del servicio (ralentizamiento), la inutilización de los servicios, la aplicación del código diseñado a la medida y la recuperación. Generalmente, este tipo de actividades son desarrolladas por personal que, en términos informáticos, son los *hackers/crackers*. Conceptos ambiguos en su etimología, pero que están relacionados con el tema de la defensa y el ataque cibernéticos.

En un sentido positivo, los *hackers* son profesionales de la informática que descubren los puntos débiles de las aplicaciones informáticas y ayudan a resolverlos. En un contexto amplio, los hackers son tecnófilos que disfrutan encontrando soluciones a tareas complejas (Rytewiki, 2021). Este tipo de expertos son los que en la mayoría de los casos orientan las actividades de ciberdefensa de las empresas y brindan asesorías en la forma como se deben emplear las actividades propias de la cibernética. En el caso del Ejército Nacional, se cuenta con personal asesor y orgánico de las unidades encargadas de este tipo de operaciones, los cuales se complementan a la hora de efectuar sus funciones.

Por otra parte, los *crackers* son personas con un vasto conocimiento que intentan vulnerar los sistemas de seguridad creados por los hackers (defensores) para cometer actos ilícitos. De este modo, aunque ambas partes son personas que tienen nociones avanzadas sobre informática, sus ideas son completamente distintas. Unos atacan ilegalmente y los otros defienden legalmente. Por todos es sabido que los hackers tienen un código ético profesional que no poseen los

crackers, que se sirven de cualquier situación y medio para conseguir su objetivo (Martínez, 2021). Estos conceptos deben ser diferenciados para que sea posible definir a cada uno y ubicarlo de acuerdo con el objetivo que se determinó para realizar los ataques o las defensas cibernéticos. En el ámbito militar reciben el nombre de *personal experto* o *ciberagentes*, que son agentes de inteligencia descritos en la Ley 1621 de 2013 y que poseen formación o pericia en el empleo de métodos y medios que describe esa ley. Esta distinción es importante porque los términos de hacker y cracker son empleados primordialmente en el ámbito civil.

El segundo tipo de operaciones que forman parte de la ciberdefensa son las operaciones de inteligencia cibernética. En síntesis, estas buscan hacer un análisis real del enemigo actual y potencial en el ciberespacio que les permita tener una apreciación de las amenazas verdaderas para el planeamiento y la conducción de las operaciones. Al igual que en la inteligencia humana, se emplea el mismo ciclo: esfuerzo de búsqueda, recolección, procesamiento, análisis, difusión y empleo del producto de inteligencia, pero encaminado al ambiente cibernético.

Por último, dentro de las operaciones de ciberdefensa se encuentra el tercer tipo de operación, las operaciones de defensa a la estructura crítica cibernética. Como su nombre lo indica, se trata de actividades para la protección, como la prevención y la mitigación de los ciberataques, la defensa activa y la aplicación de los artefactos especiales.

Ya habiendo definido los dos tipos principales de operaciones y sus subtipos, es posible esbozar las posibles aplicaciones de las operaciones ciber como soporte a las unidades de OO. EE. en Colombia. Una capacidad que en la actualidad, y gracias a la evolución de la tecnología y a la globalización, constituye un elemento de vital importancia para la desestabilización de cualquier organización, sea gubernamental o no, militar o civil.

Enlace de operaciones especiales

Antes de analizar las ventajas y desventajas que las operaciones ciber pueden brindar como soporte a las OO. EE. en Colombia, es necesario entender el funcionamiento estratégico y empleo de las unidades de FF. EE. en el país. En la historia colombiana, las FF. EE. han tenido una vital importancia en el desarrollo de los sucesos de orden público, desde la toma del Palacio de Justicia, hecho que llevó a la creación de la primera unidad de FF. EE. en el país, hasta los golpes más certeros a los cabecillas de las Fuerzas Armadas Revolucionarias de Colombia (FARC), que

lograron sentar a este grupo subversivo en las mesas de diálogos en el proceso de paz que se realizó en el año 2016.

Y no solo a nivel nacional se ha determinado la importancia de este tipo de Fuerzas. En los Estados Unidos, después del 11 de septiembre de 2001, con el atentado a las Torres Gemelas, se evidenció la relevancia de emplear las FF. EE. en la guerra contra el terrorismo. En un informe presentado al Congreso de los Estados Unidos después de las operaciones realizadas contra Osama Bin Laden en mayo de 2011 en países de Oriente Medio, se destacaba la efectividad y evolución de las Fuerzas de Operaciones Especiales tras más de diez años de lucha:

Las Fuerzas de Operaciones Especiales y los operativos de Inteligencia (elementos esenciales del tridente del poder nacional de un Estado) son las mejores fuerzas, las mejor adiestradas, las mejor equipadas y las mejor lideradas [...]. Este éxito es consecuencia directa del liderazgo del presidente Obama y de las prioridades de seguridad nacional establecidas cuando llegó a la Presidencia, así como a la luz verde que dio a las Fuerzas de Operaciones Especiales este fin de semana. (Rodríguez & Jordan, 2015, p. 108)

Debido a la situación de orden público que ha vivido nuestro país hace más de cinco décadas, la experiencia que han adquirido las FF. EE. en el Ejército Nacional las han convertido en un punto de referencia para diversos países de la región, como Brasil, Perú, México, entre otros, e inclusive en objeto de análisis en la guerra irregular en selva. Este es el caso del ejército de los Estados Unidos, que tiene un enlace del Joint Special Operation Command (JSOC) trabajando directamente en las instalaciones del Comando Conjunto de Operaciones Especiales (CCOES), para brindar asesoría, pero más que todo para captar el conocimiento que las unidades del CCOES emplean en el planeamiento y el desarrollo de OO. EE. a lo largo y ancho del país.

Este alto estándar de profesionalización se logró gracias a diversos aspectos: un exhaustivo proceso selección; un alto nivel de entrenamiento; la dotación de material de la más alta calidad; la adquisición de materiales nacionales y de países potencias mundiales en el ámbito militar; una capacidad de integración conjunta, coordinada e interagencial y, por último, el mayor bienestar que se le pueda brindar a un soldado. Gracias a la combinación de estos pilares, vistos todos dentro del ciclo de operaciones, descanso y entrenamiento (CODE), se ha logrado adquirir un *good will* que permite, en estos momentos, la exportación de esta capacidad a otros países para que sea empleada tanto en entrenamiento como en operaciones.

Un claro ejemplo de la excelencia de las FF. EE. de Colombia, a parte de los índices de efectividad en sus operaciones contra los grupos terroristas, son los campeonatos que han ganado en las diversas participaciones de Colombia en el campeonato suramericano de Fuerzas Comando realizado por el ejército de los Estados Unidos. Anualmente, en diferentes países de Latinoamérica, estas unidades compiten entre sí para obtener la victoria, para lo cual ponen a prueba capacidades distintivas de OO. EE., como asalto en áreas cerradas, pruebas de tiro, pruebas físicas, tiradores de alta precisión, pruebas de estrés, marchas de máxima exigencia, entre otras. Específicamente, Colombia posee diez títulos de las quince ocasiones en que ha participado en esta prueba, en la cual compiten alrededor de diecinueve países del continente. Cabe señalar que las Fuerzas Comando es una competencia auspiciada por el United States Southern Command (USSOUTHCOM), y dirigido por el Special Operations Command South (SOCSOUTH), cuyo objetivo es promover la cooperación regional y multinacional, la confianza mutua, la preparación e interoperabilidad de las Fuerzas de Operaciones Especiales del hemisferio occidental (García, 2019).

Dicho lo anterior, ahora es necesario analizar la doctrina de las FF. EE. para entender la aplicabilidad de las operaciones ciber en sus misiones. Entendiendo cómo operan estas unidades, es posible hacer un análisis prospectivo para determinar si es viable o no integrar la capacidad ciber a los destacamentos de las FF. EE. o si es aún mejor agregar esa capacidad a una operación determinada en la que sea requerida.

Las OO. EE. son acciones militares conducidas por unidades especialmente organizadas, entrenadas, equipadas y certificadas, con alta movilidad y flexibilidad, en espacios hostiles, negados y políticamente sensibles, para alcanzar objetivos militares de repercusiones estratégicas (Ejército Nacional de Colombia, 2017b). Este tipo de acciones militares es realizado por diversas unidades tácticas dentro del Ejército Nacional y que en su conjunto forman los Regimientos de Fuerzas Especiales (REGFE), quienes a su vez conforman la División de Fuerzas Especiales del Ejército Nacional (DIVFE), con capacidades únicas y especiales en su razón de ser.

Poseen características que son indispensables para pensar en este tipo de operaciones, como lo son objetivos estratégicos, alto riesgo de ejecución, consecuencias políticas y diplomáticas, inteligencia, planeamiento, entrenamiento, medios aéreos y comunicaciones, y se desarrollan en áreas de difícil acceso. Cuando se agrupan, complementan y cumplen a cabalidad estas características, se generan condiciones óptimas para el desarrollo y la obtención del éxito de la misión.

Pueden realizar dos tipos de capacidades críticas: la guerra especial y los ataques de precisión quirúrgica, que son capacidades que se emplean mayormente en Colombia. Las primeras son la ejecución de actividades que implican una combinación coordinada de acciones, letales y no letales, las cuales son ejecutadas por tropas de OO. EE. que cuentan con un vasto entendimiento y comprensión del ambiente operacional, dominio de idiomas extranjeros y capacidad de entrenar y combatir junto con otras formaciones de combate, en ambientes permisivos, inciertos u hostiles (Ejército Nacional de Colombia, 2017c). Este tipo de capacidad está más centrada en la facultad de despliegue de tropas especiales en ambientes externos (extranjero) para trabajar con asociados de la acción unificada. En este escenario, tienen el objetivo de desarrollar la estabilidad regional, mejorar la seguridad global y facilitar operaciones futuras, esto con la valiosa cualidad del operador especial de navegar y adaptarse a través de la cultura, las prácticas, los comportamientos y las tácticas aceptadas. Dentro de estas capacidades encontramos la guerra no convencional, la asistencia a fuerzas de seguridad, la contrainsurgencia, la preparación del ambiente operacional, la evacuación de no combatientes, la defensa interna en el extranjero, el apoyo a operaciones de información y los asuntos civiles.

Respecto a la segunda capacidad crítica, los ataques de precisión quirúrgica son acciones militares planeadas y conducidas de manera precisa, que emplean las FF. EE. con el fin de capturar, destruir, obtener o recuperar objetivos designados previamente (Ejército Nacional de Colombia, 2017b). Estas capacidades se utilizan en el desarrollo de las operaciones militares que se ejecutan en el territorio colombiano y que le han permitido a la nación asestar grandes golpes estratégicos a cabecillas de grupos terroristas, como las antiguas FARC, el Ejército de Liberación Nacional (ELN), el Grupo Armado Organizado Residual (GAOR) Clan del Golfo, entre otros.

Como parte de este tipo de capacidades, en las cuales el Ejército de Colombia es experto, se encuentra el reconocimiento especial, cuyo objetivo principal es la búsqueda de información en tiempo real a través de la vigilancia y el reconocimiento, con grupos muy pequeños infiltrados en los ambientes operacionales más adversos; la acción directa, en donde, a través del empleo del poder de fuego, se busca la neutralización de objetivos con operaciones de corta duración; el contra-terrorismo, que son todas las tácticas y técnicas empleadas para prevenir y responder a las acciones del terrorismo; el rescate de rehenes y la recuperación de personal, cuya finalidad es recuperar personal civil secuestrado en óptimas condiciones y, por último, el asalto aéreo, capacidad distintiva de las FF. EE. y en la que

poseen una gran experiencia, la cual consiste en emplear diversas técnicas para insertar las unidades en ambientes hostiles.

Teniendo claras las capacidades críticas y las operaciones distintivas de las FF. EE., ahora se puede empezar a esbozar cuáles serían las ventajas y desventajas de emplear las capacidades ciber en las Operaciones de Fuerzas Especiales.

En la organización diversa con que cuentan las unidades de FF. EE. en el Ejército Nacional y según su doctrina, la mínima organización es un destacamento de acción directa, compuesto por doce operadores especiales, o de reconocimiento especial, el cual se compone de un equipo de reconocimiento conformado por entre seis y ocho operadores especiales, cada uno de ellos con una especialidad única de acuerdo con el tipo de misión que se requiera. Se encuentran especialidades como armamento, inteligencia, comunicaciones, explosivos, sanidad y planeamiento. Precisamente son estas especialidades las que le dan el nombre de Fuerzas Especiales. Cada operador se enfoca en los conocimientos de alguna especialidad y dentro del destacamento cuenta con un reemplazo de su misma especialidad. En otras palabras, hay un primario y un secundario.

En este contexto, las operaciones ciber cabrían dentro de los conocimientos que podría tener un especialista en inteligencia, ya que en la institución estas capacidades pertenecen y son responsabilidad directa de la Inteligencia, como se analizó en los apartados anteriores. Sin embargo, lo que se debe determinar acá es la viabilidad del vasto conocimiento que debe adquirir el operador especial de inteligencia para aplicarlo en las Fuerzas de Operaciones Especiales. Dado que la cibernética es un conocimiento muy técnico y de mucha experiencia, este especialista requeriría bastante información, cursos complementarios y mucha experiencia en el manejo de tecnologías y sistemas. Además, como la prioridad de las FF. EE. es trabajar en conjunto en el desarrollo de las capacidades críticas para el cumplimiento de misiones tácticas, este operador estaría en constante entrenamiento, principalmente en el modo de crear redes de informantes en el ambiente operacional, la forma en que se va a infiltrar con fachadas y el empleo de esa información para volverla inteligencia que pueda ser accionable. Ese sería su esfuerzo principal como operador de inteligencia en las FF. EE. En consecuencia, requeriría demasiado tiempo entrenar a este especialista para que tenga reales capacidades en hackeo o en ataques ciber.

En el mundo de la informática se habla de que para llegar a ser un hacker maduro exitoso se tienen que construir unos pilares bastante sólidos de conocimientos y desarrollar habilidades excepcionales en cuanto a la programación de computadoras que permitan sortear los diferentes obstáculos que van a afrontar.

Otra de las áreas más importantes que estos profesionales deben dominar es la red de computadoras, por lo que tienen que saber cómo se entrelazan y se comunican entre sí a través del internet y las redes internas, sabiendo que tienen que estar familiarizados con los protocolos actuales y futuros en los que estas se construyen (EUROINNOVA, 2019).

Es decir, no se hace énfasis en que el operador especial de Inteligencia sea un hacker, pues la razón de la conjuntes entre las FF. EE. y las operaciones ciber no consiste en eso, sino en la capacidad que debe tener este operador en el manejo de redes, la programación y la tecnología de punta en sistemas informáticos. Esto sin contar que la tecnología informática avanza a una velocidad impresionante. La evolución tecnológica que se ha presentado en los últimos años ha sido completamente vertiginosa, hasta el punto de sacudir los conceptos más básicos. En un contexto que se ha movido a una velocidad que nadie imaginó, resulta razonable que incluso personas que se consideran expertas en tecnología o que trabajan con ella en su día a día se encuentren confusos, incapaces de apreciar la magnitud de los cambios que tiene la tecnología en su naturaleza de evolución constante (Dans, 2010).

Por lo tanto, este operador debe contar con un mínimo de habilidades que le permitan, en el momento en que sea necesario, infectar una central informática para desestabilizar o neutralizar alguna actividad del enemigo. Para ello se precisan habilidades mínimas para el ingreso a diversos sistemas y, en caso de presentarse algún bloqueo, que este especialista sea capaz de romper esa encriptación y poner en práctica la infección del sistema. Es por esto que no es viable que las capacidades de un hombre de Inteligencia ciber sean orgánicas del destacamento de FF. EE.

El punto de vista más apto y viable, de acuerdo con el análisis de las diversas variables, sería agregar esta capacidad de Inteligencia pura al destacamento de FF. EE. Al poseer un agregado en la OO. EE., sea cuál sea la capacidad crítica que se vaya a emplear, se contaría con un agente de inteligencia que poseería la capacidad real para solventar cualquier situación de informática que se le presente, y este sería protegido por el personal orgánico de la unidad de FF. EE. Se requeriría de un mínimo de entrenamiento en técnicas de movimiento, disciplina táctica y tiro en general para que este especialista de inteligencia pueda operar en conjunto con el esfuerzo principal que harían las FF. EE. De esta manera, en el momento decisivo cuando se requiera dentro de la operación, estaría en condiciones de emplear sus conocimientos en programación, redes e informáticas, para cumplir a cabalidad el objetivo de implantar el virus en determinada red. Luego de esta actividad, los operadores especiales realizarían la extracción de la unidad sana y salva, de acuerdo con el planeamiento realizado.

Entre las ventajas de tener este hacker agregado al destacamento se podrían analizar las siguientes: conocimiento profesional de sistemas, redes y programación; experiencia en el manejo complejo de sistemas y sus derivados (encriptación, claves, software, etc.); dedicación al entrenamiento de la especialidad de Inteligencia (caracterización, organización de redes, obtención de información, etc.), entre otras. Estas ventajas serían de vital importancia durante el desarrollo de una Operación Especial que requiera aplicar esta experticia bajo presión –por ejemplo bajo fuego enemigo o con el tiempo mínimo para hacer la extracción segura del personal–, poder solventar una situación en la que el sistema informático presente bloqueos o que su sistema de defensa cibernética entre en operación. Es aquí donde el agente de ciber agregado a la unidad especial debe demostrar sus conocimientos y experiencia en el manejo de sistemas de cómputo y redes.

Por esta razón se recomienda que el experto en cibernética sea un miembro de la Inteligencia (CCOCI) agregado al destacamento por el tiempo que tomen las fases de la operación, cuando se planee el despliegue de las tropas, el desarrollo de la misión táctica, la extracción y, por último y muy importante, la revista después de la acción (RDA), en donde se determina la viabilidad de continuar con la combinación de especialidades de las armas de FF. EE. e Inteligencia.

Entre las desventajas que tendría agregar esta capacidad a las FF. EE. se encuentran: dentro del destacamento se tendría un hombre que no está capacitado en el desarrollo de técnicas, tácticas y procedimientos de OO. EE., que son únicos dentro de la doctrina militar y que son de difícil alcance debido al alto nivel que poseen las FF. EE. Esto podría generar retardo en el avance, descubrimiento de la fuerza de asalto, violación de medidas de seguridad, descoordinaciones internas entre el personal, entre otras, generando vulnerabilidades y, en el caso más crítico, el fracaso de la misión con la posibilidad de pérdidas humanas y de material.

Las FF. EE. de Colombia tienen un ejemplo claro de estos riesgos, específicamente, por la muerte de un miembro del Cuerpo Técnico de Investigación (CTI) de la Fiscalía en una operación contra un cabecilla de las FARC ejecutada en el Guaviare. Luego de la entrega de armas de la Fuerza Aérea Colombiana (FAC), cuando se procedía a hacer la inserción de las tropas especiales del CCOES en el asalto aéreo, el funcionario de la Fiscalía presentó una contingencia cuando realizaba la técnica de rappel, lo que causó su caída y posterior deceso; al parecer, omitió realizar un protocolo que es necesario en estos procedimientos. Esta lamentable situación llevó a que la operación cambiara su objetivo principal, pues desde ese momento el esfuerzo principal se concentró en encontrar su cuerpo. Este ejemplo evidencia,

como se argumentó, que integrar personal no experto en los procedimientos de OO. EE. en operaciones reales conlleva un riesgo de importante consideración.

Por otra parte, los alcances operacionales que las operaciones ciber brindarían a las unidades de OO. EE. se pueden presentar en diversas situaciones reales. En el ámbito de la guerra especial y en la guerra no convencional, que son las actividades conducidas en un ambiente de conflicto orientadas a la búsqueda de Inteligencia para debilitar la capacidad de lucha del adversario en aproximación indirecta, a través de acciones tendientes a limitar sus recursos y capacidades críticas y con apoyo de recursos locales de personal y logística (Ejército Nacional de Colombia, 2017d), se evidencia que el empleo de capacidades ciber y de FF. EE. en el extranjero, en caso de requerirlas, pueden dar resultados favorables con su empleo conjunto.

Por ejemplo, insertar tropas especiales en ambientes peligrosos, a través de las líneas enemigas, con el objetivo de llegar a algún blanco estratégico. Piénsese como ilustración el caso de una central de control de una red ferroviaria, en donde el personal de las FF. EE. emplea todas las técnicas, métodos y tácticas para infiltrarse y, con el apoyo del agente experto en cibernética, poner un dispositivo en sus sistemas para infectarlos con algún tipo de virus que permita generar remotamente, desde una central aliada, un caos en el funcionamiento del transporte de trenes. En este escenario, descontrolar los horarios, las rutas, los sentidos del ferrocarril, la información de la carga que llevan los trenes, entre otras acciones, permitiría paralizar este medio de transporte, que en un conflicto sería vital para desplazar de forma rápida y económica las tropas y los medios de transporte militar pesado, además de la logística para el desarrollo de las operaciones militares.

Esto es, precisamente, lo que ha ocurrido en la guerra entre la Federación de Rusia y Ucrania en el oriente europeo, en donde un aspecto clave ha sido fortalecer la capacidad de las tropas ferroviarias, que tienen la tarea de mantener las líneas ferroviarias en buen estado de funcionamiento durante y en preparación de las operaciones de combate, así como de organizar puntos temporales de desembarque de blindados en el campo de batalla. Un conflicto anterior había mostrado la necesidad de hacer esta reforma: en la guerra ruso-georgiana del año 2008 el desempeño del sistema ferroviario fue regular, pues dejó a algunas unidades rusas con numerosos problemas relacionados con la entrega de agua potable, alimentos, combustible y municiones (Montero, 2021). Como se ve claramente, los sistemas de transporte ferroviarios tienen una importancia estratégica en cualquier tipo de conflicto de índole convencional.

Continuando con la exposición, otro de los tantos aspectos en los cuales las operaciones ciber pueden apoyar a las FF. EE. en ambientes tácticos es el daño a

los sistemas de armas, tanto terrestres como aéreos, de determinada instalación militar. Un ejemplo podría ser penetrar una instalación militar con las técnicas de las FF. EE. y, con la experticia de un hacker, neutralizar su sistema de defensa para permitir el ingreso de tropas de infantería, caballería o de aeronaves de la Aviación del Ejército Nacional o de la FAC.

Otro tipo de misión en la que se podría emplear un arma de letalidad estratégica en conjunto con el apoyo de la especialidad ciber es el ataque a fuentes de energía. La energía eléctrica es uno de los recursos estratégicos más valiosos y utilizados en la época actual, de manera que si este servicio se interrumpe, se afecta gravemente el empleo de herramientas virtuales, lo cual, a su vez, repercute en una reducción de la productividad y, por lo tanto, en grandes pérdidas monetarias para algunas industrias y empresas (Asociación Colombiana de Ingenieros de Sistemas [ACIS], 2021).

En este sentido, por ejemplo, se pueden usar los ataques cibernéticos en una planta de energía para insertar algún tipo de virus en sus sistemas y desbloquear la seguridad de sus equipos, mientras los operadores especiales ejecutan tareas de seguridad. Esto permitiría paralizar momentáneamente el país para que las fuerzas convencionales efectúen un control territorial, una operación ofensiva o una ocupación y con esto lograr una ventaja táctica sobre el terreno. Además, dado que un elemento crucial en el desarrollo normal de una civilización o una sociedad son los servicios básicos, como alimentación, transporte o servicios públicos (agua, energía, internet, telefonía, etc.), se podría alterar el orden público de determinada región y desestabilizar al gobierno opositor si se logra interrumpirlos o afectarlos mediante una operación de FF. EE.

En la situación real y actual de Colombia, en el conflicto interno que se vive principalmente contra las diferentes organizaciones guerrilleras, como el ELN o el GAOR, también se podría pensar en una operación especial de acción directa como las que se han descrito. Por ejemplo, luego de un ataque de las unidades especiales a un determinado campamento en donde se ubique un cabecilla X, se podría insertar por asalto aéreo a un ciberagente para que ingrese a los equipos de cómputo (computadores portátiles, USB, entre otros) que estuvieran en el lugar y hackear información vital, como cuentas de correos electrónicos, información financiera, ubicaciones, contactos, posibles planes terroristas a futuro, entre otras. Así, en tiempo real, podría penetrar esos sistemas informáticos y emplear la información para realizar operaciones de engaño, judicialización a personas con nexos terroristas, blanqueo de cuentas bancarias, extinción de dominio, posicionamiento de unidades en ventajas en ciertas regiones, contrainteligencia, anulación de

atentados terroristas, entre otras acciones que puede realizar la fuerza pública y otros organismos encargados de la seguridad del Estado.

Estos y muchos otros ejemplos más serían los infinitos alcances operacionales en ambientes tácticos que brindan las operaciones ciber en conjunto con las unidades de operaciones especiales. Este tipo de operaciones sería un talón de Aquiles del enemigo que se esté enfrentando en determinada situación, sea en el interior del país o en el extranjero.

El empleo de estas capacidades es frecuente en las actuales confrontaciones mundiales, en las cuales el *hard power* y el *soft power* se combinan en un ambiente de desarrollo de batallas en diversos frentes. Así lo analiza la doctrina Gerasimov, que describe la nueva forma de guerra con represalias económicas, propaganda, subversión política y operaciones psicológicas, de manera que para lograr el triunfo se debe conseguir la supremacía en el manejo de la información y la comunicación estratégica (Kowalski, 2021). Este es, precisamente, el ambiente perfecto en donde las capacidades ciber pueden brindar un soporte táctico a las unidades de OO. EE. para que, con su combinación, sea una punta de lanza para el Gobierno Nacional en temas de seguridad y defensa.

Conclusiones

El análisis realizado evidencia la importancia que tienen las operaciones ciber en la actualidad. Como su desempeño en las guerras modernas, también tienen un papel significativo tanto en la defensa como en la ofensiva de un país. Un ejemplo claro se observa en la guerra que libra la Federación de Rusia contra Ucrania, pues el empleo que han hecho los dos bandos de estas capacidades ha influido los cursos del conflicto. Desinformación a la población mundial; daño a información de estamentos del gobierno ucraniano; viralización de propaganda con técnicas sofisticadas rusas para divulgar un discurso clásico que justifica la invasión a Ucrania, entre otras acciones, son el vivo modelo de los diversos daños que pueden hacer los agentes cibernéticos.

Las FF. EE. han sido vitales en el desarrollo de las guerras desde la época Antigua –en donde no fueron identificadas como tal, aún cuando ejecutaban acciones típicas de FF. EE.–, hasta la época Moderna, en donde han neutralizado a terroristas de talla internacional como Osama Bin Laden. Estas unidades permitirán a cualquier Estado alcanzar objetivos militares estratégicos de difícil cumplimiento en las más adversas condiciones, gracias a las capacidades naturales que poseen.

La unión de estas dos capacidades, ciber y FF. EE., amplifica y potencia las opciones de éxito que un comandante requiere en el nivel estratégico. Como se pudo evidenciar en los apartados anteriores, la combinación genera muchas ventajas para el desarrollo de una misión en especial, pero también algunas desventajas, que son naturales en cualquier proceso de unificación; sin embargo, si se emplearan por separado, no sería posible pensar en el desarrollo de estas misiones críticas. Se puede determinar entonces que, en casos específicos, es de vital importancia el soporte que puede brindar las operaciones ciber a las FF. EE. en ambientes tácticos. La anulación de sistemas de seguridad, el control de comunicaciones, el soporte vital de energía a determinada región, la extracción de información para su posterior uso, operaciones de engaño, entre otras, son los múltiples usos que un comandante en el nivel estratégico puede darle a esta dupla en el nivel táctico.

La importancia del entrenamiento conjunto entre Inteligencia (ciber) y las FF. EE. radica en que esto permite disminuir las desventajas que estas acciones conllevan. El valor que tiene esta coordinación entre el agente cibernético y los operadores especiales incrementa los factores de éxito de la misión, pues la otra posibilidad, es decir, que el especialista en Inteligencia se integre como orgánico del destacamento de acción directa o dentro del equipo de reconocimiento especial, implica mucho tiempo en formación que es vital en el entrenamiento de las FF. EE.

En este sentido, continuar el estudio de este tema potencia el tridente del poder estratégico de Colombia, compuesto por su Inteligencia, ciberdefensa y las FF. EE. Por esta razón, es fundamental que en las FF. EE. y en la Inteligencia se empiece a generar doctrina sobre el empleo conjunto de estas capacidades, a través de ejercicios prácticos de planeamiento y desarrollo. Con esto se podrían empezar a cumplir objetivos militares en un posible escenario de guerra externa o interna, de manera que, con el tiempo y llegado el caso, Colombia cuente con la capacidad de enfrentar una situación real en la que sea imperativo combinar estas dos competencias estratégicas de la Fuerza para contrarrestar una amenaza latente para la nación.

En los ambientes actuales de tensión que experimenta la región, donde el empleo de todos los medios de lucha que integran la guerra híbrida son posibles, es necesario que Colombia tenga esta capacidad ciber+FF. EE. en estado de alerta, de modo que, en cualquier momento, pueda desplegarla y desarrollarla en una misión táctica con propósitos estratégicos. Con las condiciones actuales de incertidumbre y volatilidad, no resulta absurdo pensar que se puede presentar un escenario donde sea necesario usarla.

Referencias

- Aharonian, A. (2018, 4 de septiembre). La guerra de quinta generación. <https://tinyurl.com/3k284r38>
- Asociación Colombiana de Ingenieros de Sistemas [ACIS]. (2021, 13 de septiembre). La importancia de garantizar la continuidad del servicio de energía en las industrias. <https://tinyurl.com/78z8nr5j>
- Azabal, G. (2021, 25 de noviembre). Guerras híbridas: Cuando los conflictos se modernizan pero nada cambia. <https://tinyurl.com/yvdtfhyp>
- Blue Radio. (2021, 11 de junio). La historia detrás del hackeo más grande contra las Fuerzas Militares de Colombia [Video]. <https://tinyurl.com/kahtps392>
- Castells, M. (2000). Internet y la sociedad red [Lección inaugural]. Programa de Doctorado sobre la Sociedad de la Información y el Conocimiento, Universitat Oberta de Catalunya, 1999. <https://tinyurl.com/mpnphpx3>
- Centro de Doctrina del Ejército [CEDOE]. (2016). *Manual Fundamental del Ejército MFE 3-07 Estabilidad [Público]*. Publicaciones Ejército. <https://tinyurl.com/3bdvy9cd>
- Comando General de las Fuerzas Militares [CGFM]. (2016). *Manual de Ciberdefensa Conjunta para las Fuerzas Militares [Restringido]*. Imprenta y Publicaciones de las Fuerzas Militares.
- Comando General de las Fuerzas Militares [CGFM]. (2018). *Manual Fundamental Conjunto MFC 1-0 Doctrina Conjunta*. Imprenta y Publicaciones de las Fuerzas Militares. <https://doi.org/10.25062/MFC10>
- Dans, E. (2010). La evolución de la tecnología: Del ordenador a la nube. En *Todo va a cambiar: Tecnología y evolución: Adaptarse o desaparecer* (pp. 191-206). Ediciones Deusto.
- EcuRed. (2012, 30 de marzo). Ciberespacio. <https://tinyurl.com/4pvs267y>
- Ejército Nacional de Colombia. (2017a). *Manual Fundamental de Referencia del Ejército MFRE 3-07 Estabilidad [Público]*. Imprenta Ejército. <https://tinyurl.com/yfp4rmfv>
- Ejército Nacional de Colombia. (2017b). *Manual Fundamental de Referencia del Ejército MFRE 3-05 Operaciones Especiales [Público]*. Imprenta Ejército. <https://tinyurl.com/32dbw83e>
- Ejército Nacional de Colombia. (2017c). *Manual Fundamental del Ejército MFE 1-01 Doctrina [Público]*. Imprenta Militar del Ejército. <https://tinyurl.com/h8ywavpv>
- Ejército Nacional de Colombia. (2017d). *Manual Fundamental de Referencia del Ejército MFRE 3-0 Operaciones [Público]*. Imprenta Ejército. <https://tinyurl.com/ducn7tje>
- Ejército Nacional de Colombia. (2021). *Manual de Campaña del Ejército MCE 3-12 Operaciones del Ciberespacio [Restringido]*. Publicaciones Ejército.
- EUROINNOVA. (2019, 21 de enero). ¿Quieres saber qué estudiar para ser hacker? Euroinno te lo cuenta. <https://tinyurl.com/2fd5xe3n>

- Fink, K. D., Jordan, J. D., & Wells, J. E. (2014). Consideraciones para las operaciones ciber-espaciales ofensivas. *Revista Military Review*, (mayo-agosto), 24-33. <https://tinyurl.com/52sh3hrk>
- Instituto de Seguridad y Bienestar Laboral [ISBL]. (2023). ¿Qué son las infraestructuras críticas? <https://tinyurl.com/3hrs3v5x>
- Kardoudi, O. (2022, 17 de marzo). El primer “deep fake” usado en un conflicto armado muestra a Zelenski rindiéndose. *El Confidencial*. <https://tinyurl.com/yuu3d6y5>
- Kowalski, M. (2021, 10 de julio). Conflictos híbridos y la doctrina Gerasimov. <https://tinyurl.com/3f8debrj>
- La Vanguardia*. (2018, 18 de diciembre). La interferencia rusa en las elecciones de EE.UU. fue dirigida a los afroamericanos. <https://tinyurl.com/mvcr7fuh>
- Ledo, I. N. (2011). Las redes sociales [Editorial]. *Revista Venezolana de Oncología*, 23(3), 133. <https://tinyurl.com/4v46bv4s>
- Martínez, J. C. (2021, 30 de agosto). Qué diferencia hay entre un cracker y un hacker. <https://tinyurl.com/3kmy78u9>
- Montero, A. (2021, 30 de mayo). Análisis de la guerra en Ucrania desde la logística militar [Video]. YouTube. https://www.youtube.com/watch?v=2HT_7Is1sGw
- Real Academia Española de la Lengua. (2022). Tecnología. *Diccionario de la Lengua Española*. <https://tinyurl.com/2pedndwd>
- Rodríguez, R., & Jordan, J. (2015). La importancia creciente de las Fuerzas de Operaciones Especiales. *Revista UNISCI*, (38), 107-123. <https://tinyurl.com/ud5jn5fm>
- Rytewiki. (2021, 1 de febrero). Hacker. <https://tinyurl.com/56kj348u>
- Salazar, S. (2020, 9 de diciembre). ¿Qué es la doctrina militar y por qué es importante? <https://tinyurl.com/6dryzn3k>
- Sánchez Medero, G. (2009). Internet: Una herramienta para las guerras en el siglo XXI. *Revista Política y Estrategia*, (114), 224-242. <https://tinyurl.com/23979csn>
- Today's Military*. (2022). Especialistas en seguridad cibernética. <https://tinyurl.com/59m488kb>

Capítulo 8

Impacto estratégico de las operaciones de desinformación y la respuesta efectiva de las Fuerzas Militares en el siglo XXI*

DOI: <https://doi.org/10.25062/9786287602809.08>

Humberto Andrés Niño Vergara
Miguel Antonio González Martínez

Escuela Superior de Guerra "General Rafael Reyes Prieto"

Resumen: La desinformación es un recurso que se ha utilizado en diferentes momentos para afectar la estabilidad política y administrativa en una sociedad. En los niveles operacional y táctico se produce para entorpecer los procesos de las Fuerzas, específicamente para dificultar la conducción de las operaciones militares y provocar un esfuerzo mayor por parte de la Inteligencia militar en el procesamiento de información para la toma de decisiones del mando. Entre los diferentes medios utilizados en esta área, por ejemplo, se difunde información sacada de contexto, noticias falsas, se afectan los activos informáticos mediante operaciones cibernéticas, entre otros. Dado que sus efectos son disímiles, se debe analizar a partir de su impacto en cada nivel de las Fuerzas Militares para establecer una estrategia. En cualquier caso, las Fuerzas Militares requieren de fundamentos doctrinales soportados por una estructura organizacional capaz de gestionar la desinformación según el impacto en cada nivel.

Palabras clave: desinformación; doctrina; Ejército Nacional de Colombia; Fuerzas Especiales; nuevas guerras.

* Este capítulo es resultado de investigación adscrito al proyecto "Naturaleza de la guerra contemporánea. Retos y oportunidades de las Fuerzas Especiales y la Inteligencia", adscrito al Departamento Ejército de la Escuela Superior de Guerra, inscrito en la línea de investigación "Naturaleza de la guerra, terrorismo, nuevas amenazas", que forma parte del grupo de investigación Centro de Gravedad, con código COL0104976. Los puntos de vista pertenecen a los autores y no reflejan necesariamente los de las instituciones participantes.

Humberto Andrés Niño Vergara

Teniente Coronel del Ejército Nacional de Colombia. Magíster en Seguridad y Defensa Nacionales, Escuela Superior de Guerra "General Rafael Reyes Prieto", Colombia. Administrador de Empresas, Universidad Nueva Granada. Profesional en Ciencias Militares, Escuela Militar de Cadetes "General José María Córdova", Colombia.

Contacto: humberto.nino@buzonejercito.mil.co

Miguel Antonio González Martínez

Doctorando en Estudios Estratégicos, Seguridad y Defensa, Escuela Superior de Guerra "General Rafael Reyes Prieto", Colombia. Magíster en Historia, Universidad Nacional de Colombia. Profesional en Relaciones Internacionales y Estudios Políticos, Universidad Militar Nueva Granada, Colombia. Docente e investigador, Departamento Ejército, Escuela Superior de Guerra "General Rafael Reyes Prieto", y docente del Programa de Relaciones Internacionales y Estudios Políticos FAEDIS, Universidad Militar Nueva Granada, Colombia.

<https://orcid.org/0000-0002-6034-912X> - Contacto: miguel.gonzalez@esdeg.edu.co

Citación APA: Niño Vergara, H. A., & González Martínez, M. A. (2024). Impacto estratégico de las operaciones de desinformación y la respuesta efectiva de las Fuerzas Militares en el siglo XXI. En L. A. Montero Moncada & O. A. Garzón Gómez (Eds.), *Comandos: Retos de las Fuerzas Especiales e Inteligencia en la guerra contemporánea* (pp. 189-208). Sello Editorial ESDEG. <https://doi.org/10.25062/9786287602809.08>

COMANDOS: RETOS DE LAS FUERZAS ESPECIALES E INTELIGENCIA EN LA GUERRA CONTEMPORÁNEA

ISBN impreso: 978-628-7602-79-3

ISBN digital: 978-628-7602-80-9

DOI: <https://doi.org/10.25062/9786287602809>

Colección Seguridad y Defensa

Sello Editorial ESDEG

Escuela Superior de Guerra "General Rafael Reyes Prieto"

Bogotá D.C., Colombia

2024



Introducción

La desinformación surge como un fenómeno emergente en los conflictos contemporáneos que tiene impacto en la estructura social y política. Por medio de estas acciones se promueve la consecución de fines políticos y se propicia el espacio para que converjan diferentes factores que atentan contra el poder del Estado, el monopolio de la Fuerza, la estabilidad de los gobiernos y el imperio de la ley.

En el presente capítulo se analizan tres aspectos fundamentales que estructuran el hilo conductual del trabajo. Primero, el concepto y la teoría de las operaciones de desinformación y su impacto estratégico a nivel internacional. En segundo lugar, se analiza el papel de las Fuerzas Militares frente a las operaciones de desinformación, bien sea para prevenir su aparición o disipar su impacto estratégico. Finalmente, como tercer punto, se estudian los fundamentos operacionales para las Fuerzas Especiales (FF. EE.) frente a las operaciones de desinformación.

A lo largo de este recorrido se recogen los conceptos doctrinales que permitirán a las FF. EE. en Colombia entender el contexto en cual los actores armados al margen de la ley lanzan operaciones de desinformación para producir una respuesta oficial, legítima, efectiva y oportuna. Por medio de esta, se busca determinar la responsabilidad o el papel que deben desempeñar las FF. EE. en el mantenimiento del orden constitucional y la defensa del Estado, tras la influencia de otros actores que buscan desestabilizarlo.

Metodológicamente, se desarrolló una investigación de carácter cualitativo, en la cual se emplearon fuentes primarias en documentos disponibles. Según Hernández Sampieri et al. (2010), existen diversas realidades subjetivas, las cuales varían en su forma y contenido entre individuos, grupos y culturas. Por ello, el investigador cualitativo parte de la premisa de que el mundo social es “relativo” y solo puede ser

entendido desde el punto de vista de los actores estudiados. Dicho de otra forma, el mundo es construido por el investigador (Hernández et al., 2010, p. 11).

Esta perspectiva metodológica encaja con la teoría en la medida en que el capítulo dialoga con el mundo contemporáneo propio de la era posmoderna, en cuya agenda se propone desmitificar los discursos (científicos, artísticos y culturales) de la modernidad que moldearon y construyeron la realidad presente, a la vez que se asume una postura crítica frente al positivismo científico del siglo XIX. Sin duda, la incursión de la lingüística con la obra de Ferdinand de Saussure, *Curso de lingüística general* (1919), abrió una nueva perspectiva interpretativa en la forma de comprender los eventos culturales y los hechos sociales. De esta manera, muchos investigadores tomaron el estructuralismo como el marco teórico de sus investigaciones influidos por la teoría del *signo lingüístico* que propuso el lingüista francés. Posteriormente, Jacques Derrida integró la noción de la “deconstrucción” de los discursos, con lo cual dio vigencia a la lucha por la verdad: por el discurso legítimo a partir del lugar de enunciación del cual emergen.

Con estas nuevas lecturas intertextuales de la realidad, aunado al fenómeno de la globalización y su profundización con la masificación del internet, se ha allanado el camino hacia una libre interpretación en la comunicación, e incluso la incorporación de neologismos como el de la *posverdad*, el cual trae al debate, finalmente, el afán por la lucha de la verdad en un mundo cada vez más volátil, complejo, incierto y ambiguo.

La desinformación

La desinformación son actividades enfocadas en difundir información falsa, mal informar e incluso desinformar a la audiencia, potencializadas en el mundo contemporáneo por la globalización y la llegada de las tecnologías de la información y comunicaciones (TIC), las cuales facilitan el acceso y la publicación de la información, con el efecto colateral de que dificultan su control. Las redes sociales (Facebook, Twitter –ahora X–, TikTok, WhatsApp, etc.) desempeñan un papel central en este fenómeno gracias a que en los últimos años se ha democratizado el acceso a internet, de manera que la población ha encontrado en estas un vehículo expedito para comunicar ideas, pensamientos, emociones, reacciones, entre otros, a gran escala y en tiempo real, sin que exista un filtro efectivo para establecer la veracidad de la comunicación y evaluar si proviene de una fuente certificada (el caso de los *bots* –programas informáticos–). Se configura así en el marco de la

posmodernidad un fenómeno paradójico: en plena era de la información, crece la desinformación de modo exponencial a partir de la instrumentalización de amplias audiencias que abarcan diferentes sectores de la población, los cuales reciben mensajes con gran rapidez, difunden el material a un costo muy bajo y con una facilidad que burla las condiciones de veracidad.

Sociológicamente, el consumo y la propagación de material de desinformación se explica a partir de la reafirmación de la identidad de la persona, que ve en el contenido la representación de su pensamiento, sin reparar en su procedencia o realismo. Esta conducta se puede reforzar debido a los sesgos cognitivos del receptor del mensaje; por ejemplo, si una persona tiene una preferencia por una determinada corriente política, tendrá una tendencia natural a creer, sin un juicio crítico previo, las noticias que refuercen su pensamiento.

Es así como esta "revolución tecnológica" aplicada al campo de la información ha impactado en diferentes esferas de la vida pública como la cultura, la economía y la política, de manera que la desinformación afecta todo tipo de emociones que se materializan en la acción política y/o en los movimientos sociales. El ámbito militar no es ajeno a este fenómeno, pues al conducir una función primordial del Estado, su defensa y seguridad, está en constante riesgo de verse afectado por operaciones de desinformación que buscan promover la inestabilidad social y afectar al Gobierno. Por esta razón, la fuerza pública debe generar condiciones de seguridad de la información para proteger los sistemas oficiales y contrarrestar los mensajes en contra del orden institucional.

Este escenario ha promovido una transición en la estrategia de despliegue hacia una visión de las instituciones oficiales en la que, justamente, la información es uno de los ejes principales (Sierra, 2003). Al igual que los recursos naturales, el medioambiente y las personas, la información se pueden entender como un activo estratégico de los Estados, pues la mala gestión de la desinformación puede traer como consecuencia altos costos políticos, económicos, sociales, entre otros.

Un antecedente de los efectos que puede tener la desinformación se encuentra en la Guerra Fría, en la cual las dos potencias dominantes del sistema internacional emplearon todos los medios posibles para contener el avance del sistema adversario, en medio de la pugna de las fuerzas ideológicas entre capitalismo y comunismo. A la sazón, ya existía la experiencia de la propaganda que los dos bandos usaron durante la Segunda Guerra Mundial para legitimar y promover, ante la opinión pública, las acciones políticas y bélicas en el marco de la guerra. El auge y la masificación de los medios de comunicación como la prensa, la radio y el cine

tuvieron un papel trascendental en la movilización de las voluntades en contra de los adversarios en contienda.

En los años 50, las tácticas de desinformación se constituyeron en un elemento formal, con agencias especiales cuyo propósito era desprestigiar a los Estados Unidos y sus aliados en beneficio del comunismo a nivel global. Como efecto, los norteamericanos diseñaron estrategias para contrarrestar los ataques de la URSS, modificando la política exterior en torno a la información y su impacto en los países aliados, su capacidad de influir en los adversarios y desplazando el uso de la fuerza. De esta manera se consolidó la Oficina de Defensa Estratégica, cuyo objetivo era desarrollar tácticas de desinformación en las relaciones internacionales del Estado (Rodríguez, 2017).

En síntesis, la desinformación tiene el propósito de afectar la estabilidad de un Estado, para lo cual trata de deteriorar el reconocimiento y la reputación de las instituciones oficiales difundiendo mensajes de odio y/o miedo. En la actualidad, uno de los países que más ha utilizado esta estrategia es Rusia, cuya intervención se ha consolidado sobre la base de los siguientes puntos críticos:

- Realizar operaciones maliciosas en medios sociales.
- Entregar desinformación por medio de métodos tradicionales de divulgación como radio y televisión.
- Influir en la opinión pública para generar aliados que defiendan su posición y compartan sus ideas frente al adversario. Para esto han utilizado sobre todo las conferencias.
- Conducir operaciones cibernéticas para dañar la percepción de los medios de comunicación.
- Hackear y divulgar información (U. S. Department of State, 2022b).

De igual manera, al investigar qué información ha tratado de posicionar, se encontró lo siguiente:

- Rusia, por ejemplo, en el conflicto con Ucrania actúa motivado por la victimización de su adversario.
- Volver a acontecimientos históricos para estigmatizar a sus oponentes o resaltar sus acciones heroicas en el pasado.
- Criticar la cultura occidental para generar incertidumbre.
- Atacar los movimientos populares y demás expresiones de inconformismo como un acto de influencia realizado por sus adversarios militares y políticos.
- Construir realidades que favorezcan su posición, crear confusión y desmoralizar al adversario (U. S. Department of State, 2022b).

De esta manera, no solo se pretende afectar la protección de la información directamente relacionada con datos oficiales, redes financieras, plataformas que permiten el trabajo del sector público y privado, entre otros ciberdelitos, sino que además se busca controlar posibles estrategias de guerra psicológica e influir en la sociedad. El internet es un recurso a disposición tanto de la información como de la desinformación, toda vez que, por un lado, permite filtrar información a velocidades extraordinarias, y por otro, facilita operaciones de desinformación para afectar un objetivo (Sierra, 2003).

Este panorama arroja una *guerra de la información*, la cual consiste en acciones dirigidas a crear y mantener la superioridad de la información, mientras se protegen los sistemas propios. En la actualidad, este tipo de guerra presenta una amplia gama de estrategias debido a que la revolución tecnológica generó nuevas amenazas, ya que diferentes grupos y entidades oficiales pueden adquirir los medios para afectar la reputación y la estabilidad de la información, e incluso robarla, borrarla, modificarla o espiarla (López, 2007).

Entonces, esta guerra de la información alimenta un concepto de guerra que no implica el uso de una boca de fuego y que se convierte en un tipo de amenaza clásico en el campo de la guerra híbrida. En este escenario, se utilizan diferentes elementos de carácter económico, político, diplomático, entre otros, para afectar la confianza del adversario, generar condiciones sociales adversas en procura de promover manifestaciones violentas, obstaculizar la reacción de los gobiernos haciendo que su sistema de gestión sea frágil y legitimar el uso de la fuerza o, incluso, considerarla necesaria (LISA Institute, 2019). Y es de este modo que las operaciones de desinformación se convierten en una modalidad de amenaza híbrida y un potencial detonante de un conflicto convencional. En cualquier caso, su finalidad es afectar a un adversario político.

Esta amenaza híbrida va de la mano con la propaganda de guerra constante en publicaciones que buscan movilizar a las personas y desacreditar al oponente. Claramente, la propaganda de guerra, al igual que la información, ha evolucionado al ritmo de la tecnología de la información (Noguera, 2013), razón por la cual se emplean las mismas prácticas: difundir estrategias falsas y utilizar la credibilidad del público. En resumen, consiste en emplear operaciones maliciosas, utilizar la desinformación y otro tipo de mecanismos para desestabilizar al enemigo (Medina, 2022).

Como se ha visto, la desinformación es el conjunto de estrategias para generar beneficio propio y dañar a un oponente. En este sentido, la información que se entrega ya tiene un objetivo específico, razón por la cual ya está tergiversada (Ustarroz, 2021).

Otros autores definen la desinformación como la información carente de exactitud o manipulada que, en cualquier caso, es difundida con una intención maliciosa; entre esta se encuentran las noticias falsas y las historias imprecisas (Rini, 2017).

La desinformación puede ir acompañada de mensajes sensacionalistas que tienen gran acogida e impacto social; en algunos casos, también de imágenes que generan un gran efecto psicológico para provocar un sentimiento de miedo, odio, rechazo, aprobación o exaltación, según el objetivo de la operación. Este método en particular se usa desde los tiempos de la radio y se ha comprobado su poder, a tal punto que se acuñó el concepto de *infodemia* (Arteaga, 2020). Su objetivo, más allá de la victoria militar, es alcanzar el poder político aprovechando las variadas emociones que fomenta en la población. Esta modalidad ha sido ampliamente utilizada por los rusos, quienes han buscado sacar provecho de la difusión de noticias falsas y de la información manipulada para imponer su visión del mundo, someter al adversario, cumplir sus objetivos y validar su intervención militar (U. S. Department of State, 2021).

En todo caso, la finalidad de la desinformación promueve un grupo de creencias, una posición política, una imagen y el reconocimiento de una figura política o, incluso, en algunos casos, busca afectar la percepción de un adversario mediante la difusión de información. La guerra de la información se consolida sobre la base de los instintos primarios de la humanidad, los cuales desencadenan una estructura de violencia organizada (Contreras, 2001).

El impacto de estas operaciones es estratégico, en la medida en que produce alteraciones sociales porque van dirigidas a los miedos de la humanidad. Una estrategia en este sentido es generar repulsión contra el enemigo por la violación de los Derechos Humanos o afectación de valores sociales según el imaginario de cada cultura. Estas operaciones de desinformación generan incluso contenido cien por ciento falso para generar repulsión (U. S. Department of State, 2022a).

Además, uno de los aspectos que hacen que este tipo de amenazas híbridas sea tan efectivo es que los agresores permanecen en el anonimato, lo cual dificulta identificar de dónde provienen las amenazas (Arteaga, 2020). Este punto es un elemento central de la doctrina rusa, en la cual se considera fundamental el empleo de una guerra psicopolítica denominada *maskirovka*, en ruso *маскировка*, que busca engañar al enemigo con técnicas de ocultamiento, simulación y difusión de noticias falsas. De esta manera, "las prácticas de *maskirovka* a escala militar incluyen [...] manejo del lenguaje [...] así, por ejemplo, la palabra *ofensiva* ha desaparecido totalmente del vocabulario militar soviético y ha sido remplazada por eufemismos tales como *movimiento*, *salida* o *defensa*" (Antoine, 2019, p. 21).

La desinformación no solo genera un impacto en la audiencia, influyendo sus emociones y sentimientos frente a sus valores sociales y miedos, sino que también se caracteriza por su origen incierto, intención e impacto, lo cual la convierte en una herramienta poderosa a nivel internacional. Y es que se desconoce quién entrega la información, si todos los datos son falsos o si, por el contrario, hubo una tergiversación, si se sacó del contexto en el que realmente ocurrieron los hechos o si se están manipulando para favorecer un interés político determinado (Arteaga, 2020).

Normalmente, al comunicar cualquier tipo de información se enfrenta el reto de que el mensaje se reciba de la manera y con el propósito que se definió cuando se decidió hacerlo. En el ambiente militar, esto genera mayor impacto, ya que un escenario contaminado de incertidumbre, discrepancias o errores en la interpretación obstaculiza la toma de decisiones y, por lo tanto, debilita la capacidad de reacción (Guzmán, 2019).

Hay dos conceptos que inicialmente convergen en este punto: las noticias falsas o *fake news* y las operaciones maliciosas. Específicamente, las *fake news* se refieren a aquellas noticias a las que se les puede comprobar la falsedad, pero que no implican necesariamente una intención perversa, pues también pueden ser consecuencia de un mensaje mal comunicado, un error en la fuente de la información, entre otros. A diferencia de las operaciones de desinformación, las *fake news* se presentan de manera aleatoria y casi por casualidad, mientras que la desinformación se calcula en contra de un grupo y reúne esfuerzos conscientes (Paladino et al., 2021).

Además de las *fake news* hay seis tipos adicionales de desinformación: 1) sátira o parodia; 2) falsa conexión con contenido de fácil apertura; 3) contenidos engañosos que son mentiras combinadas en una serie de datos veraces; 4) falso contexto, que involucra una serie de eventos en un contexto ajeno al real; 5) contenido impostor, que es cuando buscan engañar a la audiencia para robar información u obtener un beneficio, y 6) contenido manipulado, que, como lo dice su nombre, tiene una intención clara de influir o dirigir al expectante en favorecimiento del desinformador (Doble Check, 2020).

Una de las medidas que han tomado los Estados Unidos para contener las operaciones de desinformación y protegerse de las noticias falsas ha sido socializarlas en medios oficiales con su correspondiente corrección o verificando los hechos, como se ve en la página web del Departamento de Estado. En Colombia, una iniciativa importante es la campaña VERA, impulsada por Asomédios, en la cual las emisoras radiales más importantes del país transmiten breves mensajes

en procura de desmentir noticias falsas que se han hecho virales a través de diferentes medios.

Pero, ¿qué tan efectiva puede ser esta medida en relación con la velocidad con la que las operaciones de desinformación cumplen sus objetivos? La realidad es que esto aún se desconoce, pero se aprecia la iniciativa de generar respuestas contundentes para contener los efectos adversos de la desinformación. Adicional a estos esfuerzos de personal capacitado para filtrar la información antes de que sea publicada, se requiere fomentar una cultura ciudadana para evitar la propagación de anuncios con desinformación, así como hacer un trabajo coordinado e interagencial para identificar con mayor eficiencia el contenido engañoso, rechazar su divulgación y contrarrestarlo desmintiendo el engaño.

Otro ejemplo reciente fue la situación de salud pública que generó el virus Covid-19. Para contrarrestar sus efectos, diferentes gobiernos, organizaciones internacionales y el sector privado se involucraron en campañas para promover la vacunación y desmentir la desinformación. En este contexto, la Unión Europea sustentó sus importantes esfuerzos en contra de la desinformación argumentando que el manejo correcto de la crisis de salud pública iba a tener una relación directa con el número de fallecimientos por la enfermedad (Comisión Europea, 2021).

La desinformación es un fenómeno organizado que requiere planeamiento, la disposición de una logística para lograr que el mensaje diseñado se propague y la persecución de un objetivo específico, entre otros elementos. Adicionalmente, la desinformación es un arma que se emplea contra un adversario para afectar su credibilidad, legitimidad, estabilidad y movilizar pensamientos, emociones y acciones en contra del enemigo o a favor de quien fragua la estrategia de desinformación (Rodríguez, 2017).

Además del impacto estratégico que se ha analizado hasta ahora, la desinformación es una industria que opera en más de 48 países. Diferentes actores que desconocen el objetivo final de la desinformación engrosan las cadenas de esta amenaza (Levy, 2021).

Por este motivo, la Comisión Europea presentó un plan de acción contra la desinformación que aporta algunas acciones puntuales para controlarla. Primero, mejorar las capacidades para detectar, analizar y exponer una operación de desinformación, para lo cual se requiere fortalecer la tecnología capaz de controlar, evitar e identificar de dónde proviene la noticia falsa o la desinformación en general, así como reaccionar de manera rápida para evitar la propagación de su contenido.

Segundo, es necesario fortalecer las respuestas del sector privado y del sector público en conjunto. Finalmente, y de la mano con lo anterior, se debe movilizar el

sector privado, aumentando la sensibilidad de la ciudadanía frente a los efectos de la desinformación y aumentar la posibilidad de adaptarse, aprender y desechar la información manipulada (Comisión Europea, 2018).

Una vez analizados los conceptos relacionados con la desinformación, a continuación se determina cuáles son los retos que asumen las Fuerzas Militares frente a las operaciones de desinformación en la seguridad y la defensa nacionales. Para esto se investiga la doctrina militar colombiana y se proponen algunos conceptos que den luces sobre cómo se deben orientar las capacidades de las Fuerzas Militares para mantener la ventaja ofensiva y defensiva en el terreno de las operaciones de desinformación.

Estrategia de las Fuerzas Militares ante la desinformación

La guerra de la información ha promovido un valor inmaterial especial en los ejércitos, cuya fuente radica en el poder y el conocimiento. La primera estrategia se ha encaminado a que los ejércitos desarrollen mecanismos de seguridad y defensa de su patrimonio inmaterial con programas de detección, control y prevención en la invasión y robo de su información más sensible (Sierra, 2003).

Con base en lo anterior, se conducen operaciones de información para fortalecer las capacidades de la Fuerza en la protección de sus activos de información, al tiempo que utiliza la desinformación como estrategia para su beneficio. Las acciones giran en torno a destruir los sistemas informáticos y tecnológicos del enemigo para imposibilitar su uso, interrumpir la circulación de la información, degradar su moral combativa y/o sus sistemas de mando y control; negar el acceso a información sensible; generar decepción en una audiencia frente al opuesto; conseguir información del contrario o plantar mensajes con contenido falso en su contra; influir en los expectantes para conseguir un comportamiento favorable para la Fuerza y detectar de manera temprana la intrusión a los sistemas informáticos oficiales (Andrade et al., 2011).

Las operaciones de información, que pueden ayudar a disuadir al adversario a cero costos en términos bélicos, se consolidan en el ataque, la defensa y el apoyo electrónico (Clark, 2010). De esta manera se entrega valor público a diferentes sectores de la sociedad y se ayuda a proteger diferentes aspectos de la vida pública y privada, como la información financiera, entre otras.

Después de analizar la desinformación como una estrategia en contra de los Estados, ahora es importante analizar la hoja de ruta de las Fuerzas Militares frente a esta creciente amenaza. Por un lado, la Fuerza debe hacer un esfuerzo para protegerse de estas operaciones y, por otro, debe definir estrategias militares para controlar la difusión de desinformación que pueda afectar su legitimidad, la del Estado en general y la del orden institucional. Para cumplir este objetivo, se requiere la intervención de todos los niveles operacionales que componen la fuerza pública.

Cuando se habla del nivel estratégico se hace referencia a ese grupo de personas y recursos materiales e inmateriales de los que dispone para facilitar la toma de decisiones del mando. En la parte estratégica, los altos mandos planean los medios y los recursos que se deben entregar al Ejército de combate, así como los tiempos, las fuentes y los estándares de calidad. Además, son el canal para establecer una relación directa con el Gobierno Central, promueven el cumplimiento de los objetivos nacionales ordenando las instituciones en función de estos y acatan la estrategia del Presidente como Comandante en Jefe de las Fuerzas Militares.

En el nivel operativo se recibe la información, los medios y los recursos pensados y ejecutados por el nivel estratégico, los cuales se utilizan en la realización de planes de operaciones diseñados en este nivel para garantizar la efectividad operacional. Por último, las unidades tácticas materializan el planeamiento operacional entregado por el nivel operativo. Los comandantes del nivel táctico emplean el personal, el medio y los recursos necesarios para conducir las misiones y cumplir las tareas.

Fundamentos operacionales para las Fuerzas Especiales frente a las operaciones de desinformación

Una vez se ha analizado el marco conceptual y teórico de las operaciones de desinformación, es posible establecer algunos lineamientos que pueden evidenciar en qué dirección se deben constituir los fundamentos operacionales frente a la desinformación.

Si se analiza la desinformación desde una perspectiva integral según las funciones, capacidades y alcance de los tres niveles de la fuerza pública, se puede concluir que en el nivel estratégico se requiere de medidas para mitigar el efecto de las operaciones de desinformación, sobre todo cuando estas amenazas interfieren

en la imagen institucional y la estabilidad político-administrativa. De igual manera, se requiere de la planeación de recursos materiales e inmateriales para capacitar y dotar al personal con las últimas tecnologías para detectar fuentes de información, origen de noticias falsas o ataques cibernéticos, proteger las bases de datos oficiales y todo tipo de táctica de esta especie.

Por su parte, en el nivel operativo se recopila la información de Inteligencia por medio de la cual se aproxima y caracteriza el adversario en todas sus áreas, capacidades, técnicas y tácticas (Guzmán, 2019), además de coordinar los esfuerzos para recolectar información en el nivel táctico. En este sentido, se requiere de tácticas que permitan identificar que la información obtenida sea veraz y que no contenga una intención de confundir, engañar la Fuerza o dificultar la toma de decisiones entorpeciendo sus procesos.

El reto en este punto es manejar la incertidumbre, ya que, a diferencia del nivel estratégico, más allá de intentar afectar la imagen institucional o la legitimidad del Gobierno, en este caso la desinformación tiene el poder de incidir en la toma de decisiones y el éxito operacional. En este sentido, obtener información falsa o manipulada afecta la integridad de la tropa y la capacidad de la Fuerza para obtener el éxito operacional esperado (Guzmán, 2019).

A nivel táctico, la inteligencia humana y demás técnicas para recoger información son procesos fundamentales que deben ser fuertemente entrenados en habilidades para detectar las fuentes de información, su calidad y sus posibles consecuencias. De igual manera, se deben emplear operaciones de información como medida disuasiva frente al adversario. En este caso, la desinformación obtiene las condiciones propicias para causar un impacto estratégico durante un tiempo limitado, el cual es equivalente al período en el que se mantengan las debilidades institucionales que dan cabida a una inestabilidad producida por la desinformación (Guzmán, 2019).

Un ejemplo de esto son las operaciones de apoyo a la información militar, que es una capacidad de las FF. EE. y es transversal a los tres niveles de la Fuerza. Por medio de estas se busca analizar y abordar la estrategia psicológica en el terreno operacional, así como apoyar las actividades de información de la institución, en coordinación con otras entidades y las autoridades civiles nacionales, entre otros (Ejército Nacional de Colombia, 2017).

Para proteger la Fuerza en la conducción de las operaciones, las FF. EE., en el cumplimiento de sus funciones y en el marco de sus competencias, pueden y deben soportar la seguridad de la información mediante instrumentos tecnológicos y

capacidades cibernéticas. Esta condición es fundamental, ya que cuentan con la misión para proteger esta acción en defensa de la soberanía y la independencia.

De esta manera lo establece la publicación conjunta *ADP 3-13* de los Estados Unidos sobre las operaciones de información, en la cual se determina que las operaciones militares en el ámbito de la información deben emplear de manera integrada la guerra electrónica, las operaciones de redes de computadoras, las operaciones psicológicas, las técnicas y tácticas de engaño militar y la seguridad de operaciones, de tal manera que sea posible afectar los procesos y las decisiones del adversario, a la vez que proteger su funcionamiento propio (Department of the Army, 2023).

Además, señala que la conducción de cualquier operación militar requiere unos procesos de apoyo que permitan el cumplimiento de la misión y de las tareas asignadas. En este caso, se necesita un soporte que garantice la seguridad de la información y la seguridad física, prevenir o anticipar ataques físicos, el desarrollo de operaciones de contrainteligencia y la cámara de combate (Estado Mayor Conjunto de los Estados Unidos de América, 2006).

Desde otro punto de vista, las operaciones de información requieren del fortalecimiento de las relaciones cívico-militares y la diplomacia militar para, por un lado, recolectar información veraz y afianzar los vínculos con la población civil y, por otro, para respaldar las funciones de Inteligencia y promover la conducción de operaciones con información certera que permita reducir el riesgo inherente a las Fuerzas Militares (Estado Mayor Conjunto de los Estados Unidos de América, 2006).

En el caso de Colombia, todas estas estrategias se deben alinear con la Ley de Inteligencia y los demás parámetros nacionales e internacionales que regulan la actuación de la fuerza pública. Además, las operaciones de información deben convertirse en una columna vertebral de cualquier operación militar, teniendo en cuenta que la desinformación es un recurso sutil pero muy efectivo del adversario para entorpecer la toma de decisiones, el éxito operacional, lograr la ventaja en el teatro de operaciones y fidelizar audiencias.

De esta forma surge una necesidad de soporte, la cual consiste en la capacidad de recolectar, almacenar y gestionar información en tiempo real con exactitud y pertinencia, buscando oportunidades de recolectar la que esté disponible, que sea de fácil comprensión y concisa (Estado Mayor Conjunto de los Estados Unidos de América, 2006). Esta información va a proporcionar al mando los datos necesarios para la toma de decisiones, de manera que dicha información requiere un esquema de seguridad específico para salvaguardar la vida de la tropa, los activos

estratégicos, la infraestructura y demás recursos materiales y no materiales del Estado colombiano para defender la soberanía, la independencia, la integridad del territorio y el orden constitucional.

Específicamente, la cámara de combate es un aspecto fundamental de las Fuerzas Militares, en el entendido de que se enfrenta a una serie de operaciones psicológicas en las que se cuestiona el accionar de las instituciones para mantener el imperio de la ley y el orden nacional. Esta es una herramienta para difundir las acciones de la Fuerza, su apoyo a la población civil, la atención del riesgo de desastres y las emergencias de diversa índole, el desarrollo de operaciones militares para la construcción de una paz estable, la desarticulación de estructuras criminales que violentan las comunidades, entre otras.

Además, por medio de las cámaras de combate se involucra la nación como testigo de la intercesión de la Fuerza, el uso de técnicas y tácticas protegidas por la normativa nacional e internacional, y los principios y valores característicos de la cultura militar. De esta forma se generan mecanismos para proteger la imagen institucional y como defensa jurídica frente a testimonios en contra del accionar de la fuerza pública.

En cuanto a las *fake news* o manipulación de contenido, es fundamental contar con un departamento o unidad que, desde el nivel estratégico en el cuartel general de la fuerza pública e incluso desde el Comando General de las Fuerzas Militares (CGFM), suministre directamente el contenido informativo a los medios de comunicación. De esta forma se va a proteger la legitimidad institucional y a contribuir a la defensa del orden constitucional y los valores sociales.

No obstante, la relación es cíclica e interdependiente, ya que se requiere de buena imagen y reputación para que los medios de comunicación, que en su mayoría son del sector privado y en algunos casos son independientes de cualquier forma de gobierno o poder público, estén en disposición de confiar en el contenido que emiten directamente las Fuerzas Militares.

De igual manera, es necesario determinar el tratamiento de las situaciones de crisis en las cuales se vea involucrada la credibilidad de las Fuerzas Armadas. Una situación puede afectar directamente las instituciones, pero también se puede presentar que se difunda falsa o maliciosamente mensajes que generen miedo e incertidumbre en cuanto a la seguridad y la defensa nacionales. Un ejemplo de esto podría ser un ataque por parte de un grupo ilegal o la invasión de otro país. Este tipo de contenido también se debe presentar en el concepto operacional de las FF. EE. constituidas para contener las operaciones de desinformación.

Conclusiones

La desinformación ataca los diferentes niveles de las Fuerzas Militares, torpedean sus procesos, dificultan la toma de decisiones y afectan la imagen institucional. Entre los diferentes ataques se encuentran la entrega, la publicación o el manejo de información falsa para caracterizar el adversario, lo cual dificulta el planeamiento operacional y la integridad de los miembros de la Fuerza. De igual manera, se vulneran las bases de datos oficiales, la legitimidad de las instituciones y la estabilidad político-administrativa.

Debido a lo anterior, cada nivel de la Fuerza tiene una serie de tareas específicas relacionadas con sus capacidades para responder a la desinformación. Principalmente, se habla de fortalecer las habilidades del arma de Inteligencia, por un lado, en la recolección de información para el desarrollo de operaciones militares y en la identificación de grupos al margen de la ley y su modo de operación. Por otro lado, se deben fortalecer los mecanismos de ciberdefensa y, en apoyo con las comunicaciones estratégicas, generar iniciativas en protección de la imagen institucional.

Frente a esto, las TIC han generado audiencias que reciben y transmiten el mensaje a velocidades vertiginosas. Estas audiencias, algunas veces por desconocimiento de los temas publicados, como reacción instintiva o en respuesta a unos estímulos, generan afinidad política, una dinámica entre bandos, ilegitimidad de las instituciones, entre otros comportamientos que afectan la estabilidad política y administrativa de los gobiernos.

En este sentido, se requieren unidades de FF. EE. capaces de contener ataques cibernéticos para salvaguardar la información que permite la toma de decisiones y el desarrollo de operaciones militares. Así mismo, para proteger la información audiovisual que podría ser sacada de contexto para desarrollar operaciones de desinformación en contra de la fuerza pública. Desde otro punto de vista, se necesitan operaciones especiales para determinar la fuente u origen de las noticias falsas o sacadas de contexto que buscan alterar el orden político y administrativo de la nación.

En todo caso, la fuente primaria de la desinformación la difunde o publica con la intención de afectar al adversario para genera apoyo político que rechace las creencias, posturas y/o el actuar del oponente. Los medios que las utilizan están soportados en la manipulación de las masas, para lo cual se dirigen a su sistema de creencias y en contra de sus valores sociales para generar una reacción idealmente violenta.

Este fenómeno desencadena unos eventos que ponen en crisis el sistema político y administrativo, lo cual permite que la fuente emisora del mensaje de desinformación cumpla sus fines políticos. Los efectos pueden ser tan potentes que incluso podrían desencadenar la caída de una institución, entidad o gobierno. Como resulta evidente, este nivel de fragilidad pone en riesgo a los Estados.

En tal sentido, estos retos implican una nueva área de experticia para el sector defensa y seguridad, el cual debe diseñar estrategias para controlar el impacto estratégico de las operaciones de desinformación y prevenir su aparición. Con este propósito, deben fortalecer su sistema tecnológico, las capacidades de la Fuerza en cuanto a la manipulación de herramientas tecnológicas y de la información, así como establecer tecnologías que le permitan reaccionar de la manera más eficiente posible.

Inicialmente, las FF. EE. deben desplegarse con fundamentos operacionales para proteger la información sensible de las entidades del Estado. De igual manera, deben inclinarse por la veracidad de la información produciendo contenido que contrarreste las operaciones de desinformación, para lo cual deben darle la posibilidad a los medios de comunicación de obtener constantemente datos de primera mano. De igual manera, es necesario que ingenien estrategias para evitar y contener la difusión de información incompleta, falsa y maliciosa.

Como complemento del análisis sobre los ejércitos que han tenido conflictos con otros países –por ejemplo los Estados Unidos, que han generado una doctrina funcional e implementado estas capacidades de apoyo para el desarrollo de las diferentes operaciones militares–, se deben generar unas tareas diferenciales para la FF. EE. colombianas, de manera que maximicen estos ataques físicos sobre la moral del adversario y así puedan sincronizar el planeamiento de operaciones de desinformación.

Referencias

- Andrade, W., Martínez, J. F., & Pineda, J. C. (2011). *Las operaciones de información en las guerras de información* [Trabajo de especialización, Universidad Piloto de Colombia]. Repositorio UNIPILOTO. <https://tinyurl.com/3f7vpwer>
- Antoine, F. (2019). Desinformación y “maskirovka” en la guerra psicopolítica soviética: El caso afgano. *Política Revista de Ciencia Política*, (diciembre), 129-137. <https://tinyurl.com/d8wxjc43>
- Arteaga, M. (2020a). El conflicto híbrido, una contribución para la incertidumbre. En Academia de Guerra del Ejército de Chile (Ed.), *El conflicto híbrido y sus efectos en la conducción operacional y táctica* (pp. 19-43). Centro de Estudios Estratégicos CEEAG. <https://tinyurl.com/2rbbvrfx>
- Clark, B. (2010). Las operaciones de información como elemento disuasivo para el conflicto armado. *Military Review*, (septiembre-octubre), 2-11. <https://tinyurl.com/3nt9b794>
- Comisión Europea. (2018). The 2022 Code of Practice on Disinformation. <https://tinyurl.com/4evc6mhe>
- Comisión Europea. (2021). Lucha contra la desinformación. <https://tinyurl.com/52cw4yd2>
- Contreras, F. (2001). La muerte del soldado: Hacia la deshumanización de las tecnologías de guerra. En F. Contreras & F. Sierra, *Culturas de guerra: Medios de información y violencia simbólica* (pp. 275-308). Cátedra.
- Department of the Army (2023). *ADP 3-13 Information*. <https://tinyurl.com/4bjc5n52>
- Doble Check. (2020). Fake news y otras 6 formas de desinformación [Video]. YouTube. https://www.youtube.com/watch?v=ZllaBk_8J2o
- Ejército Nacional de Colombia. (2017). *Manual Fundamental de Referencia del Ejército MFRE 3-05 Operaciones Especiales [Público]*. Imprenta Ejército. <https://tinyurl.com/32dbw83e>
- Guzmán, A. (2019). La desinformación estratégica como recurso disuasivo durante la crisis. *Revista Ensayos Militares*, 5(2), 99-114. <https://tinyurl.com/44vvvcmt>
- Hernández Sampieri, R., Fernández, C., & Baptista, L. (2010). *Metodología de la investigación* (5.a ed.). McGraw-Hill.
- Levy, G. (2021, 10 de agosto). La creciente industria de la desinformación. <https://tinyurl.com/y3dts9av>
- LISA Institute. (2019, 20 de mayo). Qué es la guerra híbrida y cómo nos afectan las amenazas híbridas. <https://tinyurl.com/258439er>
- López, C. (2007, agosto). La guerra informática. *Boletín del Centro Naval*, (817), 219-224. <https://tinyurl.com/bdcrauey>
- Medina, A (2022, 28 de enero). ¿Qué es la guerra híbrida? La estrategia de Rusia contra Ucrania. *El Debate*. <https://tinyurl.com/mtv564bt>

- Noguera, A. (2013, 20 de noviembre). *Propaganda de guerra, una estrategia adaptada al conflicto colombiano: Análisis de la propaganda de guerra empleada por Uribe y Santos para combatir los grupos guerrilleros* [Tesis de pregrado, Pontificia Universidad Javeriana]. Repositorio PUJ. <https://tinyurl.com/mzvtnc43>
- Paladino, A, Villalba, M., & Miguel, M. (2021). Entrevista a Martín Alfredo Becerra: Desinformación, fake news y posverdad. *Palabra Clave*, 10(2), e133. <https://doi.org/10.24215/18539912e133>
- Rini, R. (2017). Fake news and partisan epistemology. *Kennedy Institute of Ethics Journal*, 27(S2), 43-64. <https://doi.org/10.1353/ken.2017.0025>
- Rodríguez, A. (2017). Fundamentos del concepto de desinformación como práctica manipuladora en la comunicación política y las relaciones internacionales. *Historia y Comunicación Social*, 23(1), 231-244. <https://tinyurl.com/ykxyu2yz>
- Sierra, F. (2003). La guerra en la era de la información: Propaganda, violencia simbólica y desarrollo panóptico del sistema global de comunicación. *Sphera Publica*, (3), 253-268. <https://tinyurl.com/4bk6c97h>
- U. S. Department of State. (2021, 7 de junio). The extraordinary scope and breadth of Russian propaganda and disinformation [Global Engagement Center Counter-Disinformation Dispatches, n.º 10]. <https://tinyurl.com/3239wjvr>
- U. S. Department of State. (2022a, 13 de enero). Exploiting primal fears [Global Engagement Center Counter-Disinformation Dispatches, n.º 13]. <https://tinyurl.com/2mysnc4w>
- U. S. Department of State. (2022b, 20 de enero). Las cinco principales narrativas de desinformación en las que insiste Rusia. <https://tinyurl.com/navpzd67>
- Ustarroz, M. (2021). *Del fenómeno de la desinformación: Marco conceptual y análisis comparativo del marco legal en la Unión Europea* [Tesis de maestría, Universidad de Barcelona]. Repositorio UB. <https://tinyurl.com/zbdcyur>

Capítulo 9

Límites de la inteligencia artificial y la tecnología *big data* en el análisis de Inteligencia*

DOI: <https://doi.org/10.25062/9786287602809.09>

Jaime Andrés Naranjo Ardila

Jorge Luis Mejía Rosas

Escuela Superior de Guerra "General Rafael Reyes Prieto"

Resumen: La inteligencia artificial y el *big data* proporcionan un entorno de enseñanza y aprendizaje para el proceso de información en el análisis de inteligencia. La tecnología configura nuevos escenarios en el campo geopolítico y de seguridad y defensa, con unas características que contribuyen a generar una serie de límites que serán analizados por las agencias de seguridad del Estado. En este sentido, es importante describir la evolución que ha tenido la inteligencia artificial, puesto que los avances de la ciencia y de la tecnología se encuentran progresando rápidamente. Esta tendencia es esencial para las personas que se encargan de procesar información, ya que, por su fácil acceso, es crucial para emplear lineamientos de protección legal de datos personales. En ese orden de ideas, los desafíos de la inteligencia artificial contribuyen a generar ámbitos de innovación en tendencias de protección legal de los datos personales y en el uso de aplicaciones.

Palabras clave: análisis; artificial; inteligencia; límites; tecnología.

* Este capítulo es resultado de investigación adscrito al proyecto "*Naturaleza de la guerra contemporánea. Retos y oportunidades de las Fuerzas Especiales y la Inteligencia*", adscrito al Departamento Ejército de la Escuela Superior de Guerra, inscrito en la línea de investigación "Naturaleza de la guerra, terrorismo, nuevas amenazas", que forma parte del grupo de investigación Centro de Gravedad, con código COL0104976. Los puntos de vista pertenecen a los autores y no reflejan necesariamente los de las instituciones participantes.

Jaime Andrés Naranjo Ardila

Teniente Coronel del Ejército Nacional de Colombia. Magíster en Seguridad y Defensa Nacionales, Escuela Superior de Guerra "General Rafael Reyes Prieto", Colombia. Especialista en Conducción y Administración de Unidades Militares, y Especialista en Administración de Recursos Militares para la Defensa Nacional, Escuela de Armas y Servicios del Ejército Nacional. Diplomado en Liderazgo con Énfasis Administrativo y diplomado en Peritazgo Administrativo y Disciplinario. Profesional en Ciencias Militares, Escuela Militar de Cadetes "General José María Córdova", Colombia.

Contacto: jaime.naranjoar@buzonejercito.mil.co

Jorge Luis Mejía Rosas

Coronel (R) del Ejército Nacional de Colombia. Especialista en Inteligencia Militar, Escuela de Inteligencia y Contra Inteligencia "Brigadier General Ricardo Charry Solano". Especialista en Administración de Recursos Militares, Escuela de Armas y Servicios, y en Docencia Universitaria, Universidad Militar Nueva Granada. Profesional en Ciencias Militares y en Administración de Empresas, Escuela Militar de Cadetes "General José María Córdova", Colombia.

<https://orcid.org/0000-0003-3233-4948> - Contacto: jorge.mejia@esdeg.edu.co

Citación APA: Naranjo Ardila, J. A., & Mejía Rosas, J. L. (2024). Límites de la inteligencia artificial y la tecnología *big data* en el análisis de Inteligencia. En L. A. Montero Moncada & O. A. Garzón Gómez (Eds.), *Comandos: Retos de las Fuerzas Especiales e Inteligencia en la guerra contemporánea* (pp. 209-229). Sello Editorial ESDEG.
<https://doi.org/10.25062/9786287602809.09>

COMANDOS: RETOS DE LAS FUERZAS ESPECIALES E INTELIGENCIA EN LA GUERRA CONTEMPORÁNEA

ISBN impreso: 978-628-7602-79-3

ISBN digital: 978-628-7602-80-9

DOI: <https://doi.org/10.25062/9786287602809>

Colección Seguridad y Defensa

Sello Editorial ESDEG

Escuela Superior de Guerra "General Rafael Reyes Prieto"

Bogotá D.C., Colombia

2024



Introducción

Para nadie es un secreto que en los últimos diez años se ha producido un gran cambio tecnológico en hábitos, gustos y en cómo se adquieren las cosas o servicios. Como parte de estos avances, actualmente existen innovaciones tecnológicas que pueden ser aplicadas en el campo de la inteligencia militar, como la inteligencia artificial (IA), el internet de las cosas, la realidad virtual, la red de bloques, las app, el *e-commerce*, el *big data*, entre otras enfocadas en la necesidad de los clientes, pero que hasta ahora no se están aprovechando. En efecto, la IA optimiza los procesos de recolección de información generando un sistema integral de control de datos, el cual facilitará el desempeño organizacional y le permitirá a la Fuerza crear una serie de habilidades, acuerdos y compromisos en torno a la ciencia de la inteligencia militar.

El presente capítulo tiene el objetivo de analizar el empleo de la inteligencia artificial (IA) y la tecnología *big data* en la Inteligencia militar para el planeamiento en Operaciones Especiales (OO. EE.). En primer lugar, se examina el desarrollo tecnológico que afecta la Inteligencia militar y las Fuerzas Especiales (FF. EE.), teniendo en cuenta que la innovación facilita la recolección de datos de forma segura mediante un código criptográfico que hasta el día de hoy no ha podido ser vulnerado. En este sentido, el capítulo propone que es necesario definir un planeamiento que facilite la adopción de medidas prospectivas para no improvisar frente a una amenaza de alto riesgo. De esta manera, se considera que el uso del *big data* y la inteligencia artificial contribuye a prevenir, controlar y mitigar los impactos y también el respeto por la anonimización de los datos personales.

Este proceso debe incorporar “la minería de datos y la *big data*”, pues si no se tienen en cuenta las variables y las expectativas de todas las partes interesadas con las que interactúa la organización, no podrá cumplir sus objetivos ni metas, de

allí que en esta fase sea muy importante realizar control y seguimiento para garantizar que el plan sea realista.

En segundo lugar, se relaciona la inteligencia artificial y la tecnológica del *big data* para la inteligencia humana en las OO. EE. Con base en el análisis, se sugiere que es necesario implementar procesos y procedimientos que ayuden a la organización a posicionarse de la mejor forma. Para cumplir este objetivo, la inteligencia artificial resulta una opción viable, ya que permite encadenar todos los procesos que son realizados de forma automatizada, establecer un modelo que genere resultados eficientes y, por lo tanto, mejorar el proceso de recolección de información. Esto permite identificar las características, costumbres, preferencias, procedimientos, comportamiento y desarrollo de las personas y las organizaciones.

Finalmente, se analiza el papel de la tecnología de *big data* para el mejoramiento continuo como tendencia de un entorno globalizado, para lo cual se sugiere analizar todo tipo de buenas prácticas gerenciales.

Antecedentes

Las primeras aplicaciones móviles datan de finales de los años 90, cuando ya estaban implícitas en los computadores. Un ejemplo claro fue la agenda en *Windows 95*, que empezó como una aplicación que enviaba señales de alerta, o los *arcade games* ("juegos de celular"), que fueron tendencia en esa época, cuyos productores encontraron un nicho de mercado (Bonami et al., 2020).

De acuerdo con Ahedo y Danvila (2014), la evolución de las aplicaciones continuó con los editores de *ringtone* ("tono de celular"), que efectuaban funciones muy básicas y su diseño era suficientemente escueto. A partir de este punto, el desarrollo de las apps se aceleró gracias a las innovaciones en tecnología, lo cual estuvo soportado por los grandes avances de los celulares, pues las compañías que los producían generaron prácticas de ventaja competitiva.

De hecho, comienza una revolución en la creación de las apps, los juegos, las noticias, el diseño, el arte, la fotografía y la medicina, todo en las manos de los usuarios gracias a los procesos acelerados de innovación de las aplicaciones móviles (Fernández, 2020). Simultáneamente, el internet creaba un sinnúmero de herramientas de muy alta calidad dirigidas hacia la innovación con el uso de las Tecnologías de la Información y las Comunicaciones (TIC), mediante las cuales garantizaba el acceso personalizado a los datos y, de esta manera, brindó al ciudadano la posibilidad de identificar las debilidades y las fortalezas de la gestión pública.

Esto fue resulta evidente en el manejo de la pandemia por coronavirus (Fernández, 2020), cuando se discutió públicamente que estas innovaciones podrían llegar a vulnerar las normas en materia del derecho al *habeas data*, ya que recolectan y centralizan la información de los usuarios por medio de la ubicación de sus datos personales. Aunque son utilizados con fines netamente estadísticos de salud, estos datos se encuentran centralizados para informar a las demás personas (Navarro, 2014).

Por lo tanto, si bien esta información puede ser empleada para verificarla con las centrales de información, también pueden servir para localizar a la persona en tiempo real con fines delictivos. Por lo tanto, como señala Daza (2020),

es muy importante no simplificar, polarizar ni reducir la cuestión a una renuncia a la privacidad para mantener la vida o la salud, o para evitar los confinamientos y otras restricciones de nuestras libertades. Las lesiones de la privacidad, como el coronavirus, no se ven ni se sienten hasta que ya es tarde. Por ello, si se plantea el debate en estos términos maximalistas, nadie apostaría por la privacidad. (p. 12)

El aprendizaje es otro campo en el que la IA adquiere sentido, ya que en la actualidad existen aplicaciones que, por ejemplo, convierten los mapas en escenarios de tres dimensiones (3D) cuando se mira con un dispositivo móvil o una cámara web. Aunque estas aplicaciones responden a la necesidad de averiguar el estado de salud de las personas, identificar riesgos e incluir alarmas o estados de alerta, es claro que estos avances tecnológicos conducen a un escenario que trasciende el nivel de información, por cuanto despliegan funcionalidades con características invasivas (Orozco, 2003).

Evolución en la concepción y el planeamiento de escenarios de guerra o confrontaciones híbridas contemporáneas

Actualmente, la evolución de las confrontaciones en el sistema internacional ha hecho invisible al adversario debido al uso de las tecnologías, lo cual implica todo tipo de retos para las sociedades modernas. Esto resulta muy notorio en lo que se refiere al establecimiento de mecanismos de seguridad y defensa, así como de políticas públicas que puedan cumplir con los intereses nacionales, ya que ahora

existe una serie de riesgos a la tranquilidad y la convivencia armónica de los pueblos. La importancia de este tema resulta evidente cuando se tiene en cuenta la llegada de nuevos actores con capacidad para desestabilizar las instituciones con el ánimo de lograr sus intereses, amparados en el marco de la economía ilegal y por encima de los objetivos de un Estado (Valencia et al., 2019).

En ese contexto, la evolución de la tecnología ha permitido el avance de la IA, la cual ha obtenido resultados en diferentes campos de acción de la sociedad, pues ha incrementado la capacidad para tomar decisiones ante sucesos inesperados gracias a la información que consiguen y procesan las máquinas. Esto crea escenarios con alto riesgo para la existencia de la humanidad, pues países como Estados Unidos, Rusia y China han revolucionado su estrategia de seguridad nacional con los recursos que les brinda la IA para proteger sus intereses nacionales en tiempos de conflictos armados o tareas de mantenimiento de la paz.

Históricamente, los fenómenos de globalización fueron cambiando progresivamente los métodos para definir una estrategia de seguridad nacional, de manera que se apostó por instaurar áreas de crisis, normalización y estabilización, todas ellas con el propósito de contribuir con el establecimiento de la paz. En este contexto, la seguridad de los Estados fue evolucionando con el paso de los años y tuvo un gran salto con los atentados del 11 de septiembre de 2001 a las Torres Gemelas en Nueva York, pues este suceso evidenció que habían emergido nuevas amenazas a la seguridad global, las cuales tenían diferentes técnicas de actuar y atacar. Como resultado, las agencias de Inteligencia de los Estados cambiaron y se prepararon empleando la tecnología como medio para obtener sus resultados.

En efecto, se encuentra que los principales desarrollos de la IA se producen en los Estados que son potencias mundiales, tanto en sus políticas de seguridad y defensa, como en la materialización de sus planes estratégicos. No obstante, el hecho de que esta tecnología se emplee en escenarios muy diversos crea la posibilidad de que surjan serias amenazas, algunas de carácter tecnológico y otras de origen humano. Según los expertos, una de estas amenazas es que la IA se convierta en autosuficiente o superinteligente, de manera que supere las capacidades de los seres humanos, y la otra es que sea empleada con fines letales o perversos contra otros Estados o actores no estatales.

La autosuficiencia de la IA, es decir, cuando supera al hombre en todos sus aspectos inteligibles, ya ha sido contemplada por la ciencia y se ha denominado "la gran singularidad". Esta postura fue argumentada por Stephen Hawking, quien manifestó abiertamente que este tipo de tecnologías podría significar el fin de la

humanidad. Por su parte, Nick Bostrom (2016), catedrático de la Universidad de Oxford, considera que la IA puede reemplazar en cierta forma el trabajo intelectual de los seres humanos, por ejemplo, realizando mejores análisis. Por eso afirma que este tipo de tecnología debe tener valores humanos y actuar de forma coordinada con todos los actores de la sociedad para lograr buenos resultados; de lo contrario, advierte Bostrom (2016), el escenario sería catastrófico e irreversible para la humanidad.

Desde una visión más moderada, el Dr. Ramón López, director de IA en España, manifiesta que una súper IA todavía se encuentra lejos de la realidad y, por lo tanto, la idea de que este tipo de tecnología podría dominar el mundo carece de fundamento científico, ya que para materializar la gran singularidad es necesario que se produzca la evolución tecnológica correspondiente (Pérez, 2023). Otros expertos señalan que si existiera una IA con mejor nivel intelectual, nunca podrá ser superior al del ser humano, pues no tiene una interacción similar con el entorno. No obstante, estas reflexiones hacen evidente que se debe analizar a fondo todo tipo de dilemas éticos, fundamentalmente respecto al uso de las armas autónomas (Valls, 2018).

Ahora bien, respecto a la IA utilizada para actividades criminales, Sonia Pacheco (citada por Rubio, 2018), directora del Business World Congress, señala que puede generar gran afectación por los riesgos a la seguridad y defensa de un Estado. En ese sentido, considera que se debe distinguir entre el mal uso de la IA “no intencionado” y el mal uso “con intencionalidad”, como la utilización de drones con objetivos terroristas o manipular las contiendas electorales usando cuentas con algoritmos en redes sociales que facilitan la automatización de mensajes, denominadas *bots*, que realizan tareas repetitivas las 24 horas del día. Un ejemplo de este uso malintencionado de la IA es el ataque a bases militares en Siria por actores no estatales o la invención de armas autónomas que son letales (Rubio, 2018).

La inteligencia artificial, componente estratégico de defensa de un Estado

La IA es una tecnología que se puede considerar bien como un componente desequilibrante en el uso de las Fuerzas Militares, o bien como un instrumento disruptivo en todos los campos de acción de la sociedad, económico, industrial o social. La capacidad de carácter geoeconómico y geopolítico que genera esta tecnología afecta directamente el contexto estratégico internacional porque facilita la toma de

decisiones y la construcción de la estrategia de seguridad nacional, pues permite ponderar el mejor curso de acción mediante la evaluación de las variables más críticas. Aunque su empleo depende de las capacidades que tengan los Estados, actualmente es un mecanismo que han integrado grandes potencias como Estados Unidos, Rusia, entre otros.

Por lo tanto, la evolución de la IA es un componente vital en la seguridad nacional, el cual contribuye a generar políticas internas que tienen amplia relación con las consideraciones expuestas por la comunidad internacional. Esta tecnología goza de gran aceptación, a tal punto que en 2017 China estableció una política de Estado bastante ambiciosa con un programa tecnológico prospectivo (2030) para posicionarse como líder mundial en este campo, para lo cual orientó sus esfuerzos en las aplicaciones de IA. De esta manera, comenzó una carrera global por tener la hegemonía en este ámbito tecnológico, según señala un informe del Foro Económico Mundial publicado en 2018, el cual proyectó que la inversión en IA alcanzará los 127 mil millones de dólares en el año 2025.

En ese sentido, es importante analizar el concepto estratégico de la IA y el fundamento por el cual los Estados invierten grandes sumas de dinero. Específicamente, el contexto es que el mundo actual se encuentra en constante evolución, las grandes potencias quieren alcanzar el liderazgo tecnológico y militar, compitiendo por la jerarquización internacional y por proteger sus intereses nacionales.

En efecto, es importante para los Estados que emplean la IA conformar una política exterior multilateral debido a las diferentes amenazas que se ciernen en el entorno global, como son: el impacto que genera el cambio climático, las armas de destrucción masiva, las crisis financieras, las pandemias, entre otros. Como se observa, es evidente la necesidad de crear e implementar mecanismos de cooperación que puedan unir esfuerzos de manera multidimensional.

Del mismo modo, el uso de la IA resulta significativo para, por ejemplo, combatir las pandemias y la pobreza multidimensional, o consolidar los compromisos internacionales orientados a mejorar su infraestructura de transporte. Cuanto más desarrollo económico y social haya, aumentan la calidad de vida de las personas y la demanda por mejorar la protección ambiental, de manera que potencie su participación dentro de las dinámicas del comercio global.

En este contexto cabe señalar que la cadena de bloques optimiza los procesos de IA en la seguridad y defensa de un Estado, pues facilita un mayor manejo de la información en pro de los intereses nacionales. Además, contribuye a emplear metodologías contables en el desempeño organizacional que le permite generar

una serie de habilidades, acuerdos y compromisos en el uso de estos ámbitos tecnológicos, aunque siempre con limitaciones a la protección de datos, la reserva y la confidencialidad (Martínez, 2019).

A su vez, esta tendencia de la cadena de bloques facilita el almacenamiento de datos de forma segura mediante un código criptográfico que hasta el día de hoy no ha podido ser vulnerado. Los mecanismos para controlar dicha información está creciendo bajo un marco de globalización y de evolución tecnológica en torno a la aldea global, lo cual evidencia que las empresas enfrentan ciertos riesgos que pueden afectar su sostenibilidad y rentabilidad.

Medios empleados en el planeamiento y la ejecución de escenarios de guerra o confrontaciones híbridas contemporáneas

En el planeamiento se realizan todo tipo de metodologías que comprenden procedimientos sistemáticos, un paso a paso que lleva a tomar una serie de decisiones que pueden generar un resultado en el campo militar. Específicamente, los estados finales deseados se definen por medio de un estudio del ambiente operacional, de manera que están conexos entre sí para emplear las capacidades de las unidades militares, entre las cuales se encuentra la optimización de la IA para tomar una posición de ventaja relativa sobre el adversario y otras amenazas. Esas tareas se encuentran desde la acción decisiva y promueven unas maniobras ofensivas (Bonami & Dala, 2020).

Teniendo en cuenta los nuevos desafíos en seguridad y defensa existentes, la Fuerza Conjunta está llamada a realizar todo tipo de actividades mediante el empleo de la inteligencia artificial, en asociación con el desarrollo de operaciones militares, para crear una ventaja y una capacidad estratégica que le permita ser más eficaz frente a las amenazas actuales y las tendencias en seguridad global (Hueso, 2019).

Por lo tanto, el uso de tecnologías de IA no solo es importante para tener movimiento y maniobra, pues potencian la integración de la seguridad y defensa del país con la finalidad de lograr un solo esfuerzo en la consolidación de los territorios, sino también en las operaciones militares, las cuales buscan obtener una posición de ventaja relativa frente alguna amenaza que atente contra la vida y la dignidad de los colombianos (Bravo, 2010).

De esta manera, además, el empleo de la IA permite neutralizar las principales estructuras de los Grupos Armados Organizados (GAO) mediante reconocimientos aéreos para identificar las posiciones de las columnas móviles y con labores de Inteligencia (humanas y técnicas) sobre el enemigo. Esto hizo posible que entre 2018 y 2022 el Gobierno fuera efectivo en la disminución de actividades como el secuestro, los homicidios y todo tipo de hechos ilícitos. Esta política de Estado, como se convirtió, muestra la importancia de que las instituciones “ocupen” todas las regiones nacionales y contribuye al desempeño de la sociedad para erradicar las desigualdades sociales que enfrenta el país (Galindo, 2005).

En efecto, el planeamiento es la combinación continua y simultánea de las actividades de las Fuerzas Militares y en la doctrina constituye uno de los primeros componentes fundamentales de las capacidades. Esto simboliza la conversión de las nuevas estructuras organizacionales de la institución en procura de ejercer estrategias de transformación y renovación, la nueva visión, el despertar y la transformación prospectiva en el entrenamiento y fortalecimiento de las capacidades. En este sentido, las Operaciones Terrestres Unificadas (OTU) permiten obtener la iniciativa y una posición de ventaja frente a los múltiples generadores de violencia, con una serie de operaciones ofensivas y defensivas, así como trabajando la conjuntes desde un enfoque interinstitucional o internacional.

Los profesionales militares aplican el arte del movimiento y la maniobra mediante el entrenamiento y la táctica, contenidos en la intención del comandante, por medio de la elección entre opciones conectadas:

- Tipos de tareas ofensivas o defensivas que describen las maniobras y tareas tácticas de misión.
- Organización para el combate de fuerzas disponibles, para incluir la distribución de recursos limitados.
- Elección fundamental de las medidas de control.
- Tiempo (antes, durante y después) de la operación.
- Desafíos y retos que el comandante está dispuesto a asumir (Vigevano, 2021).

Este elemento es de vital importancia para fortalecer la cooperación entre Colombia y sus aliados, teniendo en cuenta que la Inteligencia estratégica y la Contrainteligencia de Estado son factores de vital importancia para la toma de decisiones. Además, se debe considerar que existen elementos externos que influyen directamente en la política exterior colombiana, por lo cual este factor contribuirá para el cumplimiento de los fines esenciales del Estado:

- Desde el carácter estratégico, se pueden fortalecer las relaciones de las agencias de Inteligencia de Colombia con sus aliados, desarrollando actividades de inteligencia estratégica y contrainteligencia para proteger los intereses nacionales, con el fin de generar mayor control frente a los crímenes transnacionales.
- Desde el carácter operacional, la inteligencia militar se puede fortalecer en sus capacidades y medios con el principal propósito de poder generar operaciones coordinadas que afecten directamente a las organizaciones armadas ilegales que delinquen en las zonas de frontera.

En ese orden de ideas, el ciclo de Inteligencia dentro de un contexto de guerra híbrida debe ser definido como el conjunto de habilidades y destrezas que, por medio del empleo de la IA, permiten estudiar los factores económicos, políticos y sociales. Estos componentes, que actúan de forma integral, potencian el poder de combate con la finalidad de obtener una ventaja militar e iniciativa para contrarrestar todo tipo de amenazas que atenten la soberanía de una política del Estado. Actualmente, la aplicación de todas las intervenciones se basa en una gestión de programas sensibles a los conflictos y con un enfoque transversal con los temas de equidad, además se presta especial atención a la creación de soluciones sostenibles y formas de intervención, una de las cuales es la Inteligencia militar involucrando la mayor participación posible.

Escenarios de confrontación híbrida aplicados a Colombia en el contexto de una confrontación hegemónica y regional

Actualmente, existe una carrera armamentística para obtener la hegemonía mundial, donde los protagonistas son Estados Unidos, China y Rusia. Estos Estados conocen la importancia que tiene mejorar sus sistemas de IA para materializar sus intereses nacionales, lo cual ha sido denominado por la comunidad académica como la *guerra fría de la inteligencia artificial*. Un ejemplo claro es China, que ha establecido dentro de sus planes de desarrollo una fuerte inversión de aproximadamente 150 mil millones de dólares en tecnología, de tal forma que realizan estrategias prospectivas que les permitan, en un futuro no lejano, ser líderes mundiales en IA y constituirse como el centro de la innovación global.

Sin duda, frente a las anteriores revoluciones económicas y sociales, el desarrollo de la IA, además de dinámica, es universal, en la medida en que garantiza conexiones simultáneas y permanentes que son la base de la llamada globalización, pues incide a escala global en las actividades económicas, comerciales, políticas y sociales, la acumulación de capital, la generación y la transmisión del conocimiento y la gestión de la información.

Del mismo modo, después de la Revolución Industrial y con la llegada de la producción en masa, la automatización y la robótica, la "industria 4.0" ya es considerada como la "Cuarta Revolución Industrial", debido a su potencial y beneficios relacionados con la integración, la innovación y la autonomía de los procesos. Los conceptos de industria 4.0 y manufactura inteligente son relativamente nuevos y contemplan la introducción de las tecnologías digitales en la industria de la fabricación. Es decir, la incorporación al ambiente de manufactura de tecnologías como el internet de las cosas, el cómputo móvil, la nube, el *big data*, las redes de sensores inalámbricos, los sistemas embebidos, los dispositivos móviles, entre otros (Valencia et al., 2019).

Sin embargo, existen objetivos que ayudan a mejorar los procesos de información con el empleo de las fuentes abiertas. Un claro ejemplo es que estas tecnologías propician situaciones en las que los individuos pueden desplegar su capacidad de colaboración, integrarse a grupos y hallar el espíritu de equipo para obtener un método de recolección de información valiosa dentro de grandes flujos de información. Como se evidencia, estas características tecnológicas permiten educar a largo plazo.

En este sentido, para que el proceso de la información en la IA sea integral se requiere una serie de especialidades –perfilamiento de identidades, análisis situacional sistémico, prospectiva, entre otras– muy particulares que ayudan a determinar una representación propia del ser humano, en la medida en que determinan características de unificación, consolidación, comunicación y actividades decisivas para que la conjunción entre la IA y la inteligencia se lleve a cabo de manera controlada. En este aspecto es en el cual la cadena de bloques contribuye a que la información digital sea distribuida, pero no copiada, lo cual se puede explicar con un ejemplo claro: una hoja de cálculo que está duplicada miles de veces a través de una red de computadoras. Luego esa misma red está diseñada para actualizar regularmente esta hoja de cálculo y con ello se produce la cadena de bloques (Palomo-Zurdo, 2018, pp. 11-23).

Actualmente, en el entorno cibernético existe una gran variedad de programas de recolección de información, no solo académica sino también de datos precisos en la función pública de un Estado. Por consiguiente, hay programas que se basan en organizar la información de personas según la empresa en donde trabajan, la ubicación de su domicilio, la afinidad en los intereses o gustos, entre otros aspectos relevantes para recoger datos importantes (Navarro, 2014). Algunos de los programas de fuentes abiertas más utilizados son:

- *Shodan*: un investigador que localiza computadoras, webcams, impresoras y distintos dispositivos electrónicos.
- *Namechk*: demuestra si un nombre de usuario está disponible en más de 150 servicios *online*.
- *Tineye*: es un explorador que parte de una fotografía y muestra en qué sitios web se encuentra (Navarro, 2014).
- *Pipl*: explorador de personas que las relaciona con distintas redes sociales y vínculos en internet.
- *Domaintools*: es un servicio que permite identificar, monitorear, buscar y analizar un nombre de dominio.
- *Tagboard*: permite analizar distintos *hashtags* o etiquetas de Twitter (ahora X).
- *Twopcharts*: es un instrumento que analiza todo lo que se publica en Twitter, admite conocer los *likes*, el cronograma e historial de publicaciones, listas y contenido relevante.
- *Foca*: es un programa que permite extraer y analizar los metadatos a distintos tipos de documentos (Arcos, 2015). Al conocer los metadatos, se puede saber quién los creó o modificó, el tipo de software que lo generó y la distinta información relacionada con un archivo (Rosales, 2005).
- *Metapicz*: permite extraer los metadatos a fotografías y con esto conocer distinto tipo de información, como qué cámara, software, fechas y teléfono fueron utilizados.

En ese sentido, la realidad es que las organizaciones no pueden permitirse esperar tanto tiempo en una era donde las intrusiones de ciberseguridad ocurren en instantes, pues la seguridad de una organización depende de una rápida identificación y acciones de respuesta. Por ello se plantea este interrogante: ¿Cómo puede un país como Inglaterra, con procesos sólidos de seguridad de la información, mejorar las capacidades para identificar “adversarios avanzados” en los sistemas y

red? La respuesta se evidencia en que, últimamente, las organizaciones han intentado generar todo tipo de procesos de forma proactiva, y a la vez, han optimizado sus estructuras e instituciones ciber y de IA. (Chipuxi & Paucar, 2020).

El papel de las Fuerzas Especiales con el uso de la inteligencia artificial como herramienta de estrategia

El proceso de automatización y monitoreo por medio de sensores tiene una función muy significativa y necesaria para el soldado de las FF. EE. en el ambiente operacional actual. La IA cada vez toma más fuerza para extraer todo tipo de información meteorológica, sobre el estado físico y de salud del personal, así como de las capacidades de un soldado en tiempo real para tomar las mejores decisiones. Además, con respecto al adversario, permite conocer su armamento, identificar sus estrategias y analizar sus cursos de acción para atacar o defender con base en una serie de patrones suministrados por los grandes servidores, entre otros aspectos de suma relevancia.

Por lo tanto, para desarrollar el máximo potencial de la IA es fundamental la interconexión, es decir, el intercambio de información constante entre varios sistemas para que cada uno pueda reaccionar ante una posible amenaza. Sin embargo, para eso es evidente que los protocolos de acceso a este tipo de datos deben ser robustos, de forma que no exista ningún tipo de pérdida y para evitar intromisiones enemigas.

A su vez, la IA facilita la toma de decisiones gracias a que hace posible ponerle sensores al soldado para conocer su estado físico y emocional, a los vehículos y a los sistemas, tomar aerofotografías, así como tener audio y video del ambiente operacional, lo cual proporciona una gran cantidad de información valiosa. Generalmente, el noventa por ciento de las operaciones especiales (OO. EE.) consiste en planear y establecer las estrategias, los puntos de control, la ubicación del enemigo, entre otros aspectos de suma importancia. De acuerdo con el General Clarke, Comandante del Comando de Operaciones Especiales de los Estados Unidos, la mayoría de los líderes militares, específicamente los que agrupan las FF. EE., concentran la mayor parte de su tiempo en el planeamiento (Barceló, 2001).

Por ende, los ejércitos modernos con FF. EE. deben instalar nuevas estructuras organizacionales que contengan tecnología IA para escanear todo tipo de

computadoras y teléfonos celulares; recopilar y contrarrestar los mensajes que deja el adversario en las redes sociales y sus tendencias; analizar de forma detallada la situación y los intereses u objetivos del enemigo, y brindar un centro de operaciones para contrarrestar todo tipo de fanatismo y extremismo violento que quiera desestabilizar los entes gubernamentales (Palomo-Zurdo, 2018).

A su vez, la IA debe ayudar a detectar las amenazas electromagnéticas. Por ejemplo, los drones diseñados con esta tecnología y aprendizaje autónomo tienen la posibilidad de seleccionar los objetivos y realizar una acción directa de fuego. Estas operaciones deben estar bajo la supervisión de un asesor jurídico operacional para tomar la mejor decisión en ámbitos legales, siempre protegiendo la integridad de los encargados de hacer cumplir la ley. En este sentido, el control humano sobre este tipo de máquinas es esencial para garantizar la protección humanitaria y un control legal efectivo.

Al respecto, cabe señalar que el Departamento de Defensa de los Estados Unidos, en la Directiva N.º 3000.09, del 12 de noviembre de 2012, define las armas autónomas como

[...] un sistema que, una vez activado, puede seleccionar y enfrentarse a objetivos sin la intervención de un operador humano. Esto incluye los sistemas de armas autónomos supervisados por humanos que están diseñados para permitir a los operadores anular el sistema automático, pero pueden seleccionar y atacar objetivos sin mayor intervención humana después de su activación. (Departamento de Defensa de Estados Unidos, 2012, p. 13)

En ese orden de ideas, los sistemas de armas autónomos sin control humano es un instrumento que selecciona y ataca objetivos de acuerdo con criterios que han establecido los ingenieros de programación y con unas reglas operacionales, pero no pueden ser detenidos por la intervención humana después de que se ha lanzado el ataque. Cabe señalar que actualmente existen más de 380 armas semiautónomas que fueron desarrolladas por Israel, China, Estados Unidos y otros países (Sossa & Reyes, 2021).

Aunque no han sido empleadas en conflictos armados, se espera que en un futuro no muy lejano se puedan utilizar con el desarrollo de la robótica y la IA, para lo cual los países desarrollados, especialmente las potencias, destinan importantes recursos financieros al campo militar, de manera que la sustitución de soldados por tecnología no parece un escenario lejano (Acosta, 2020).

Ahora bien, todo sistema automático de armas no es necesariamente un sistema totalmente autónomo, ya que la intervención humana en la programación debe respetar todo tipo de parámetros exigidos por la ley, en la medida que requiere el uso de un operador. Actualmente, muchos armamentos militares poseen grandes niveles de automatización y tienen la capacidad de ser semiautomáticos, por ejemplo los drones, que pueden realizar actividades de forma automática, como despegar y aterrizar, sin la necesidad de que sea dirigido por un ser humano gracias a las rutas que se programan con el Global Position System (GPS).

En el caso de Estados Unidos, gran parte del presupuesto que destina a la defensa lo enfoca en desarrollar IA, lo cual le ha permitido tener una ventaja significativa respecto a China, sus principal competidor. Específicamente, estas tecnologías se relacionan con los siguientes campos:

- *Operaciones no tripuladas*: incluye los sistemas aéreos, terrestres o marinos tanto de superficie, como de inmersión con sistemas no tripulados y cada vez más autónomos.
- *Operaciones navales y aéreas a grandes distancias*: mediante bases expedicionarias flotantes o a través de aviones cisterna no tripulados que permitan aumentar significativamente el radio de acción de los aparatos de las Fuerzas de los Estados Unidos sin depender de aliados poco fiables (Vigevano, 2021).
- *Operaciones no-observables*: comprende las tecnologías furtivas que van mucho más allá de la "invisibilidad" al radar. Aspectos como la composición del material, la pintura, las emisiones infrarrojas y muchos otros factores complican la invisibilidad a niveles insospechados (Gutiérrez, 2014).
- *Guerra submarina*: es otro de los campos dominados por los Estados Unidos, pero China está construyendo submarinos no tripulados que serían capaces de llevar a cabo ataques de estilo kamikaze contra buques enemigos.
- *Ingeniería e integración de sistemas*: es la clave de todo el edificio militar estadounidense. Consiste en un sistema de sistemas, centrado en nuevos niveles de cooperación interarmas dentro de cada ejército e interejércitos dentro del conjunto de sus fuerzas armadas, que permite un mayor control sobre el campo de batalla.

Por lo tanto, es significativo que muchos países hayan creado todo tipo de marcos jurídicos para regular la protección de datos personales, ya que con el empleo de la IA y la disponibilidad de *big data* existe el riesgo de que se vulnere la información del titular de los datos, por ejemplo la suplantación o la creación de perfiles exactos para generar todo tipo de extorsiones; para fines políticos ilegales

o lo que se denomina *guerra cognitiva*, es decir, hacerles crear a las masas una serie de eventos catastróficos por las decisiones de sus gobernantes sin ningún tipo de criterio u objetividad.

En resumen, la estrategia de los Estados Unidos se enfoca en sobrepasar los avances chinos con la finalidad de salvaguardar a los combatientes humanos, para lo cual desarrolla sistemas aéreos, navales y terrestres no tripulados controlados a distancia e incluso autónomos que tengan la capacidad del factor sorpresa y puedan atacar en cualquier lugar y momento a partir del desarrollo de una red global de observación y ataque (Acosta et al., 2020).

En ese orden de ideas, los nuevos escenarios tecnológicos han demostrado que la protección a la vida privada y a los datos personales pueden ser vulnerados de diferentes formas. Esto no afecta solamente a un país, sino también a millones de personas en todo el mundo, pues traspasa los límites fronterizos, como sucedió recientemente en el campo geopolítico electoral con Cambridge Analytica. Esta compañía se especializa en aplicar test a una gran cantidad de personas con el interés de enviar mensajes personalizados para influir sus gustos en el ámbito comercial y electoral, de manera que los ciudadanos consuman determinados productos u orienten su intención de voto a favor de un candidato. El caso más emblemático sucedió en las elecciones presidenciales de los Estados Unidos en las que fue elegido Donald Trump (Hill & Dance, 2020). Estos eventos señalan la necesidad de establecer una serie de límites que deben ser analizados por las agencias de seguridad del Estado.

Ahora bien, las tecnologías de IA son un recurso más a disposición del personal encargado de analizar y procesar la información, el cual facilita la creación colectiva de conocimiento por su fácil acceso. Sin embargo, es importante establecer lineamientos para proteger legalmente los datos personales para que los resultados de estos análisis no caigan en manos criminales o de corporaciones que los vulneren flagrantemente para intereses electorales o comerciales. En ese sentido, la IA y el *big data* pueden proporcionar un entorno de enseñanza y aprendizaje para el análisis de la información que se realiza en los procesos de inteligencia.

En definitiva, los nuevos retos y desafíos de la IA contribuyen a generar ámbitos de innovación para crear todo tipo de tendencias. En el campo militar, la IA y el *big data* permiten enlazar las bases de datos de información de los usuarios, con el fin de analizar y determinar la solución o acción correctiva entre realizar seguimiento entre lo planeado vs lo ejecutado para asegurar el cumplimiento de los objetivos. Por estas razones, cada día cobra mayor fuerza la necesidad de establecer lineamientos para la protección legal de los datos personales en el uso de aplicaciones.

Conclusiones

La IA y la tecnología *big data* en el análisis de la información son conceptos determinantes en el proceso de Inteligencia. Esto se debe tener en cuenta en los diferentes niveles del planeamiento estratégico, pues el empleo de estas capacidades puede afectar el ambiente operacional y la toma de decisiones, en especial el planeamiento de la gran estrategia. De igual forma, el uso de IA y *big data* hace que las capacidades de Inteligencia se especialicen y actualicen cada vez más para hacer análisis lo más aproximado a la realidad, en la medida en que permiten formular escenarios de futuro más concretos frente a este nuevo desafío.

Del mismo modo, es importante determinar las variables y expectativas que tienen todas las partes con las que se interactúa para establecer su veracidad y credibilidad, de manera que sea posible concretar los objetivos y evaluar cuáles metas tienen una mayor posibilidad de ser cumplidas. Por lo anterior, es necesario desarrollar más sistemas efectivos de control y seguimiento para facilitar que el planeamiento se ajuste mejor a la realidad.

Dado que el desarrollo de la innovación y la tecnología, la IA y el *big data* pueden tener propósitos positivos o negativos, existe la posibilidad de que sean usados para generar ventajas que permitan explotar situaciones favorables ajustadas a la verdad o al engaño. En ese orden de ideas, la utilización de la IA y la tecnología *big data* en el planeamiento y la ejecución de escenarios de guerra o confrontaciones híbridas contemporáneas tienen una importancia determinante en la toma de decisiones, ya que se realizan como un conjunto de tareas y métodos conexos entre sí que comprometen el empleo de las Fuerzas y diferentes campos del poder para tomar una posición de ventaja relativa sobre el adversario, las amenazas y los factores de inestabilidad.

En este sentido, la Inteligencia militar se fortalece cuando incrementa sus capacidades y medios con el propósito de generar más inteligencia. Al realizar un mejor proceso de análisis con la ayuda de estas herramientas, los tomadores de decisiones pueden planear mejor operaciones coordinadas que faciliten el cumplimiento de la misión y el estado final deseado en los diferentes teatros o áreas de operaciones internas y externas.

Por esta razón se debe estar al tanto de la revolución que generan estas tecnologías, pues si se usan, por ejemplo, para desarrollar una IA que muestre el centro de gravedad del adversario, puede multiplicar la ventaja, hacer que las decisiones sobre la ejecución de las operaciones sea más eficiente y reducir al mínimo posible

las acciones del recurso humano, pero haciéndolas más letales. Asimismo, las tecnologías armamentistas, por más desarrolladas que sean, se vuelven vulnerables si se logra impactar con audacia las variables que constituyen las fortalezas de un Estado, de forma que se transformen en una desventaja en el área de injerencia o en su misma área.

Actualmente, el mundo está apuntando a los desarrollos tecnológicos de todo tipo, se ha ido transformando a través de las crisis y, por lo tanto, ha tenido que innovar para supervivir, lo cual hace necesario, para bien o para mal, cambiar el pensamiento porque el mundo real está pasando al virtual. Desde el punto de vista estratégico, la IA y la tecnología *big data* fortalecerán las relaciones de las agencias de Inteligencia, de manera que desarrollarán tareas de inteligencia estratégica y contrainteligencia para neutralizar las amenazas comunes y proteger los intereses nacionales, con el fin de generar mayor control. En cuanto al carácter operacional, la Inteligencia militar debe desarrollar acuerdos para fortalecer sus capacidades y medios, con el propósito de generar operaciones coordinadas que afecten directamente a las organizaciones armadas ilegales que delinquen en el territorio nacional.

No obstante, se debe indicar que si no se establece algún tipo de regulación jurídica para usar y desarrollar la IA, se puede abrir una peligrosa puerta a una serie de actividades criminales y a graves vulneraciones a los Derechos Humanos. En este contexto, se debe recordar la distinción entre un mal uso de la IA “no intencionado” y el mal uso “con intencionalidad”, por ejemplo con fines terroristas, lo cual representa un riesgo a la seguridad y la defensa nacionales (Romero, 2019). Por lo tanto, para limitar estas amenazas es fundamental establecer un marco jurídico internacional y vinculante que regule esta tecnología.

En el contexto actual de guerra híbrida, emplear la IA en el estudio de los factores económicos, políticos y sociales que potencian directamente el poder de combate, permitirá realizar de forma integral las tareas, obtener una ventaja militar y, de esta manera, ganar la iniciativa para neutralizar todo tipo de amenazas que atenten contra la soberanía y las políticas de Estado. En ese sentido, contar con estas herramientas permite tener un enfoque transversal en el desarrollo de las operaciones que preste especial atención a la participación de la Inteligencia militar.

Finalmente, la IA y el *big data* son instrumentos que siempre deberán depender del análisis y el control de una persona, quien debe determinar qué sirve y qué no en el planeamiento. Por lo tanto, también es fundamental que cuente con un marco jurídico que lo regule y con la asesoría adecuada para blindar todas las decisiones que tome cuando incorpore dichas tecnologías.

Referencias

- Acosta, A., Aguilar-Esteva, V., Carreño, R., Patiño, M., Patiño, J., & Martínez, M. (2020). Nuevas tecnologías como factor de cambio ante los retos de la inteligencia artificial y la sociedad del conocimiento. *Revista Espacios*, 41(05), 25-32. <https://tinyurl.com/35d-m93jd>
- Ahedo Ruiz, J., & Danvila del Valle, I. (2014). Las nuevas tecnologías como herramientas que facilitan la educación. En J. Días-Cuesta (Ed.), *Estrategias innovadoras para la docencia dialógica y virtual* (pp. 25-40). ACCI.
- Arcos, R. (2015). Reservas de inteligencia: Una comunidad ampliada de inteligencia. *Inteligencia y Seguridad*, (8), 11-38. <https://tinyurl.com/yc77ra2d>
- Barceló, M. (2001). A.I. (inteligencia artificial). *Byte España*, (78), 98-99. <https://tinyurl.com/32x36khf>
- Bonami, P., Piazzentini, L., & Dala-Possa, A. (2020). Educación, big data e inteligencia artificial: Metodologías mixtas en plataformas digitales. *Comunicar*, 65(25), 43-52. <https://doi.org/10.3916/C65-2020-04>
- Bostrom, N. (2016). *Superinteligencia: Caminos, peligros, estrategias*. Teell.
- Bravo, G. (2010). El proceso de inteligencia, vigilancia, adquisición de blancos y reconocimiento. *Revismar*, (1), 58-64. <https://tinyurl.com/3w85dju>
- Chipuxi, V., & Paucar, J. (2020). *Propuesta de un modelo de cadena de suministro basado en tecnología Blockchain* [Tesis de pregrado, Universidad Central del Ecuador]. Repositorio UCE. <https://tinyurl.com/yc6t2h4b>
- Daza, M. (2020). *Grado de conocimiento y nivel de implementación de la tecnología Blockchain en empresas colombianas* [Tesis de maestría, Pontificia Universidad Javeriana]. Repositorio PUJ. <https://tinyurl.com/bdv3w9ys>
- Departamento de Defensa de Estados Unidos. (2012). DOD Directive 3000.09, "Autonomy in Weapon System". <https://tinyurl.com/466nkb9b>
- Fernández, M. (2020). *Tecnología Blockchain en la logística portuaria* [Tesis de pregrado, Universidad de Cantabria]. Repositorio UNICAN. <https://tinyurl.com/vhh4ztb3>
- Galindo, C. (2005). De la seguridad nacional a la seguridad democrática: Nuevos problemas, viejos esquemas. *Estudios Socio-Jurídicos*, (7), 496-543. <https://tinyurl.com/2vh6a55c>
- Gutiérrez Abarzúa, H. (2014). El concepto ISTAR: ¿Una herramienta válida para la función de inteligencia de las Fuerzas Militares del siglo XXI? *Revista Fuerzas Armadas*, (230), 55-63. <https://doi.org/10.25062/0120-0631.859>
- Hill, K., & Dance, G. (2020, 10 de febrero). Una aplicación de reconocimiento facial ha identificado a víctimas de abuso infantil. <https://tinyurl.com/2m3tj3yd>
- Hueso, L. (2019). Riesgos e impactos del big data, la inteligencia artificial y la robótica: Enfoques, modelos y principios de la respuesta del derecho. *Revista General de Derecho Administrativo*, (50), 1-37.

- Martínez Devia, A. (2019). La inteligencia artificial, el big data y la era digital: ¿Una amenaza para los datos personales? *Revista La Propiedad Inmaterial*, (27), 5-23. <https://doi.org/10.18601/16571959.n27.01>
- Ministerio de Tecnologías de la Información y Comunicaciones. (2016). Investigación, desarrollo e innovación. *Ciberseguridad*, 10-12. <https://tinyurl.com/5xkx5k6b>
- Navarro Bonilla, D. (2014). El ciclo de inteligencia y sus límites: Producción de información. *Cuadernos Constitucionales de la Cátedra Fadrique Furió Ceriol*, (48), 51-65. <https://tinyurl.com/58yw8ncj>
- Orozco, L. E. (2003). La calidad de la universidad: Más allá de toda ambigüedad. <https://tinyurl.com/9rsx47tj>
- Palomo-Zurdo, R. J. (2018). Blockchain: La descentralización del poder y su aplicación en la defensa. *Boletín IEEE*, (10), 885-904. <https://tinyurl.com/2s43yc2y>
- Pashchuk, Y. (2013). *Medios de implementación de Instar en el sistema de Inteligencia de las Fuerzas de Ucrania*. Universidad Nacional de la Fuerza Aérea (KNAFU). <https://tinyurl.com/y5d6ujv8>
- Pérez, J. (2023). Ramón López de Mántaras, experto en inteligencia artificial: "La IA sola no resolverá absolutamente nada. Serán los humanos". *Diario El País*, <https://tinyurl.com/52vwc9m2>
- Romero, S. (2019). Inteligencia artificial como herramienta de estrategia y seguridad para defensa de los Estados. *Revista de la Escuela Superior de Guerra Naval del Perú ESUP*, 16(1). <https://tinyurl.com/56a4vwah>
- Rosales Pardo, I. R. (2005). La inteligencia en los procesos de toma de decisiones en la seguridad y defensa. *Cuadernos de Estrategia*, (130), 39-64. <https://tinyurl.com/2u9yczne>
- Rubio, I. (2018, 15 de noviembre). Necesitamos la inteligencia artificial para sobrevivir como especie. <https://tinyurl.com/4yy47rz2>
- Sarda, J. M. (2016, 22 de septiembre). *En la inteligencia de un Estado se pueden mostrar varios tipos de amenazas a las estructuras organizacionales del mismo que pueden afectar los procesos de información. Toma de decisiones y manejo de amenazas*. Universidad de Valencia.
- Sossa Azuela, H., & Reyes Cortés, F. (2021). *Inteligencia artificial aplicada a robótica y automatización*. Marcombo; Alfaomega.
- Valencia Bermúdez, M. P., Puerta Bohada, J. S., Collazos Ballén, N., Urrea, D., & Cañas C. (2019). Influencia de la cuarta revolución industrial en Colombia. *Punto de Vista*, 10(16), 1-18 <https://doi.org/10.15765/pdv.v11i16.1419>
- Valls, M. (2018). La inteligencia artificial y su encaje en las estrategias de seguridad nacional. *Boletín IEEE*, (12), 472-485. <https://tinyurl.com/4y38fw4c>
- Vigevano, M. (2021). Inteligencia artificial aplicable a los conflictos armados: Límites jurídicos y éticos. *Arbor*, 197(800), Artículo e600. <https://tinyurl.com/s73rua84>

Capítulo 10

La geopolítica del crimen organizado en el orden mundial 2.0: un estudio de caso*

DOI: <https://doi.org/10.25062/9786287602809.10>

Pedro Alexis Ortiz Celis

Escuela Superior de Guerra "General Rafael Reyes Prieto"

Fabio Albergaria

Escuela de Defensa de Brasil

Resumen: El objetivo del capítulo es analizar de manera general los actores y factores que intervienen en operaciones de inestabilidad en el orden mundial 2.0. Asimismo, analiza e identifica algunas características y elementos que participan en el desarrollo de operaciones de inestabilidad generadas especialmente en el Subcomplejo de Seguridad del Norte Andino y cuyas externalidades repercuten en el sistema internacional desde el nivel de análisis regional. Para eso se contextualizan las ilícitas transnacionales como una variable generadora de inestabilidades y se estudia cuál es el papel del espacio andino-amazónico en esas dinámicas.

Palabras clave: amenazas; factores de inestabilidad; ilícitos transnacionales; operaciones de inestabilidad; seguridad.

* Este capítulo es resultado de investigación adscrito al proyecto "Naturaleza de la guerra contemporánea. Retos y oportunidades de las Fuerzas Especiales y la Inteligencia", adscrito al Departamento Ejército de la Escuela Superior de Guerra, inscrito en la línea de investigación "Naturaleza de la guerra, terrorismo, nuevas amenazas", que forma parte del grupo de investigación Centro de Gravedad, con código COL0104976. Los puntos de vista pertenecen a los autores y no reflejan necesariamente los de las instituciones participantes.

Pedro Alexis Ortiz Celis

Teniente Coronel del Ejército Nacional de Colombia. Magíster en Estrategia y Geopolítica, Escuela Superior de Guerra "General Rafael Reyes Prieto", Colombia. Magíster en Artes y Ciencias Militares, WINSEC. Especialista en Administración y Conducción de Unidades Militares, Escuela de Armas y Servicios del Ejército Nacional. Especialista en Administración de Recursos Militares para la Defensa Nacional, Escuela de Logística del Ejército. Profesional en Ciencias Militares, Escuela Militar de Cadetes "General José María Córdova", Colombia. Contacto: pedro.ortizce@buzonejercito.mil.co

Fabio Albergaria

DoctoryposdoctorenRelacionesInternacionalesyposdoctorenEstudiosLatinoamericanos, Universidad de Brasilia. Magíster en Desarrollo Sostenible. Profesor asistente de la Escuela Superior de Defensa (ESD). Contacto: fabio.queiroz@defesa.gov.br

Citación APA: Ortiz Celis, P. A., & Albergaria, F. (2024). La geopolítica del crimen organizado en el orden mundial 2.0: un estudio de caso. En L. A. Montero Moncada & O. A. Garzón Gómez (Eds.), *Comandos: Retos de las Fuerzas Especiales e Inteligencia en la guerra contemporánea* (pp. 231-256). Sello Editorial ESDEG.
<https://doi.org/10.25062/9786287602809.10>

COMANDOS: RETOS DE LAS FUERZAS ESPECIALES E INTELIGENCIA EN LA GUERRA CONTEMPORÁNEA

ISBN impreso: 978-628-7602-79-3

ISBN digital: 978-628-7602-80-9

DOI: <https://doi.org/10.25062/9786287602809>

Colección Seguridad y Defensa

Sello Editorial ESDEG

Escuela Superior de Guerra "General Rafael Reyes Prieto"

Bogotá D.C., Colombia

2024



Introducción

En la definición clásica, el sistema internacional es el conjunto constituido por unidades políticas que tienen unas con otras relaciones regulares, y que eventualmente son susceptibles de ser implicadas en una guerra general (Aron, 1963). Todavía, después de casi tres décadas desde el final de la Guerra Fría y la rigidez bipolar, existen muchas incertidumbres sobre la naturaleza del actual sistema internacional.

De esa manera, en este complejo sistema en el que los destinos de sus actores se entrelazan en un contexto propicio para conexiones del más variado orden, somos llevados a un escenario que aún no es predecible, abierto a nuevas posibilidades, entre las cuales se encuentra definir una agenda de seguridad más adecuada a los nuevos tiempos y prioridades de las relaciones internacionales, incluso en el caso de América del Sur.

En otras palabras, como señala Queiroz (2022), las amenazas superpuestas, desde fuera y dentro de una región, demandan respuestas coordinadas para proteger a los intereses de quienes, en cierta medida, se ven afectados por las externalidades producidas por asuntos como: la degradación del medioambiente; el cambio climático; los desplazamientos forzados inducidos por conflictos; la radicalización y la financiación del terrorismo; los ciberataques en gran escala; el uso intencional de la violencia por entidades no estatales; y, para los efectos de esta investigación, la proliferación de Estados fallidos y el crimen organizado.

Esa es la interpretación de Haass (2008), quien define el sistema internacional actual como “la era de la no polaridad”, un mundo dominado no por un concierto tradicional de Estados, sino por una miríada de actores, muchos de ellos no estatales y dotados de importantes recursos de poder. En estos términos, Haass define la no polaridad, que se decanta en esta difusión de poder, como la principal

característica del sistema internacional en el siglo XXI; en sus palabras, un cambio tectónico en relación con las visiones sistémicas tradicionales del pasado reciente.

En el sistema no polar de Haass, el poder de los Estados se diluye a medida que se producen flujos transfronterizos del más variado orden (drogas, información, armas, bienes, personas) fuera del conocimiento y el control de las estructuras gubernamentales. En consecuencia, estos mismos flujos posibilitan la actuación de otros actores, ocupando espacios antes restringidos al monopolio de la acción estatal. Así, el mundo no polar tiene el potencial de dar lugar a un escenario peligroso, propenso a un “desorden no polar”, que aumenta en número de amenazas y vulnerabilidades.

En otra perspectiva, Viola y Leis (2007) sostienen que hemos vivido en lo que ellos llamaron sistema internacional con hegemonía de las democracias de mercado, y que tiene su fuerza estructural fundamental en la globalización, marcada por la transición de la sociedad industrial a la sociedad del conocimiento, intensiva en información.

En ese escenario, los principales actores estatales que relacionan economías de libre mercado y regímenes democráticos definen su política exterior y de defensa de forma que no representen, en relación con cualquier otro país de este centro, amenazas a sus intereses vitales. Por lo tanto, es importante destacar que Viola y Leis (2007) definen como regímenes democráticos aquellos que presentan: la existencia del gobierno de la ley (*rule of law*), elecciones libres y competitivas, diferenciación clara entre gobierno y oposición, alternancia en el poder, derechos y garantías individuales frente al Estado, separación entre los poderes, garantía constitucional de las minorías y protección de la sociedad contra una eventual apropiación excesiva de recursos por parte de la clase política.

A partir de eso, los autores señalan que las principales amenazas al actual sistema de seguridad internacional son: 1) el terrorismo transnacional asociado al radicalismo islámico; 2) la proliferación de armas de destrucción masiva; 3) los Estados que desafían activamente este sistema de seguridad, como Irán y Corea del Norte; 4) los Estados que desafían parcialmente este sistema de seguridad y que tienen recursos de poder, como China y Rusia, y 5) el crimen transnacional.

A su vez, Zakaria (2008) entiende que la dinámica del sistema internacional está definida por lo que llamó el “ascenso del resto”. Si bien, en su evaluación, a nivel político-militar el mundo sigue siendo unipolar, bajo la hegemonía norteamericana, en las demás esferas –industrial, económica, financiera, social y cultural– se produce un cambio significativo en la distribución del poder a favor de otras

potencias, entre las cuales destacan China e India, así como de actores no estatales, lo cual indica que existe una superposición de elementos de unipolaridad y multipolaridad.

En síntesis, estas lecturas confirman las conclusiones de un informe elaborado en 2004 por una comisión de expertos nombrada por Kofi Annan, entonces secretario general de la Organización de las Naciones Unidas (ONU), en que se identificaron seis fuentes principales de amenazas o desafíos a la agenda de seguridad contemporánea: 1) guerras entre Estados; 2) violencia dentro de los Estados, guerras civiles, violaciones a gran escala de los Derechos Humanos y genocidio; 3) pobreza, enfermedades infecciosas y deterioro ambiental; 4) armas nucleares, radio-lógicas, químicas y biológicas; 5) terrorismo, y 6) crimen organizado transnacional.

Estos enfoques, que representan solo una pequeña muestra de los esfuerzos emprendidos en la lectura de las relaciones internacionales en esta primera década del siglo XXI, denotan la reconfiguración de fuerzas del sistema internacional contemporáneo en sus diversos niveles de análisis, desde el sistémico hasta el regional. Y, en ese sistema, el crimen transnacional contribuye, como vimos, a formar escenarios de inestabilidad cuyas externalidades no son plenamente conocidas en su capacidad de generar rupturas.

En otras palabras, como bien observa Zakaria (2008), esta nueva realidad global profundamente alterada tanto por la inclusión de temas no convencionales en la agenda internacional de seguridad, como por la creciente y significativa actuación de actores no estatales, destaca la imperiosa necesidad *"to construct a new approach for a new era, one that responds to a global system in which power is far more diffuse than ever before and in which everyone feels empowered"*. Es decir, dejamos atrás un mundo bipolar y peligroso, pero previsible, ya que estaba basado en el riesgo calculable de un juego entre dos adversarios, hacia otro, de contornos indefinidos, que implica antiguos riesgos, es verdad, pero también inéditas posibilidades (Queiroz, 2013). ¡Es el orden mundial 2.0!

Lo anterior resulta más claro si se considera también la perspectiva de Buzan y Waeber (2003), según la cual en el contexto de la posguerra fría, el ámbito regional es el espacio en que se expresan y reflejan, de manera más evidente e inmediata, las dinámicas de inseguridad resultantes de las interacciones que se establecen entre los diversos actores y sectores en que interactúan. En cuanto a América del Sur, según los mismos autores, si el Cono Sur optó, desde los años 1990, por el camino de la integración y el fortalecimiento de la confianza mutua teniendo el Mercosur como pilar, el Norte Andino-Amazónico –nuestro universo de análisis–,

a su vez, mantiene latentes las reminiscencias de un pasado de conflictos y rivalidades en un escenario agravado por problemas estructurales endémicos.

Así, en una situación de creciente inestabilidad y de muchas preguntas sobre el futuro del orden global, sostenemos esta hipótesis relacional directa: cuanto más transnacionales sean las acciones de los ilícitos, mayor será la probabilidad de que el llamado Subcomplejo de Seguridad del Norte Andino y, más específicamente, el espacio Andino-Amazónico, se convierta estructuralmente en un arco de inestabilidad basado en la fragilidad del Estado de Derecho y en la economía de los ilícitos.

Metodología

Para recopilar los datos que permiten probar la hipótesis se empleó el *desk research*, técnica que consiste en hacer un amplio levantamiento del material publicado en relación con el objeto de estudio. Con este propósito se analizaron documentos de fuentes públicas oficiales relevantes (como ministerios, Fuerzas Armadas y servicios de inteligencia) y también material mediático, como periódicos, revistas y sitios de internet especializados.

En cuanto a la ontología de la investigación, elegimos dinámicas de inestabilidad en el contexto del orden mundial 2.0 como parámetro para definir el universo de análisis y, como complemento, el modelo descriptivo de los Complejos Regionales de Seguridad (CRS), en general, y de los Subcomplejos Regionales de Seguridad (SRS), en específico, los cuales se explican en el tópico dedicado al marco conceptual.

Así las cosas, este estudio de caso utilizó una metodología cualitativa para responder a la pregunta de investigación. De esa manera, se realiza un análisis con el fin de proveer inferencias descriptivas (cómo) y causales (por qué) sobre la geopolítica del crimen organizado en la triple frontera norte (Brasil-Colombia y Perú), en lo que entendemos como uno Arco de Inestabilidad Andino-Amazónico en progreso.

Luego, este trabajo es también, por la naturaleza del objeto de investigación, un estudio exploratorio, por ser un tema poco frecuente en la literatura, especialmente en cuanto a su interpretación a la luz de los marcos conceptuales seleccionados.

Finalmente, para responder a la pregunta de investigación con el fin de llegar a respuestas que confirmen o refuten la hipótesis planteada, se sigue una cadena causal que enumera las variables seleccionadas para el estudio, es decir: 1) las variables independientes, que son aquellas que afectan a otras variables y son fenómenos útiles para explicar las características o comportamiento del objeto de

estudio; 2) la variable dependiente, que es lo que el investigador quiere explicar en términos de la influencia de una o más variables independientes y, finalmente, 3) la variable interviniente, que es aquella que, en una secuencia causal, se ubica entre la variable independiente y la variable dependiente, de manera que ayuda a explicar el proceso por el cual la primera influye en la segunda.

El orden mundial 2.0

Según Richard Haass (2017), ya no vivimos más en el orden mundial 1.0, construido en torno a la protección y las prerrogativas exclusivas de los Estados desde la Paz de Westfalia (1648), sino que habitamos un mundo integrado e interdependiente o, en otras palabras, en el orden mundial 2.0. En ese escenario, casi toda y cualquier cosa, amenazas y/o personas pueden llegar a cualquier lugar, estableciendo así complejas relaciones de interdependencia. Luego, en el orden mundial 2.0 “lo que ocurre en el interior de un país ya no puede considerarse asunto exclusivo de ese país” (Haass, 2017, p. 2), de manera que las amenazas superpuestas procedentes del exterior y del interior de una región dada o país exigen respuestas coordinadas para proteger a los intereses de aquellos que son, en alguna medida, impactados por las externalidades resultantes.

Esa es la situación de los ilícitos que han permeado muchas de las instituciones del Estado, incluso en América del Sur, por medio del crimen organizado transnacional. Este fenómeno se apoya en algunos de los elementos que definen el orden mundial 2.0, entre los cuales se encuentran: la apertura comercial, el flujo de bienes y personas, el desarrollo tecnológico y el tránsito de agentes no estatales que comercializan tales productos, fenómenos que generan, entonces, ciclos de inestabilidad y retos al Estado de Derecho, como se presenta en el siguiente apartado.

El escenario internacional está determinado por la interdependencia, situación que se ha visualizado críticamente en las diversas amenazas que actualmente azotan a las naciones. Como se ha mencionado, si bien la guerra en su concepto clásico westfaliano está en retirada, no ha sido obstáculo para que se sucedan actos terroristas como los atentados perpetrados en Nueva York y Washington D.C. el 11 de septiembre de 2001. Esto evidencia “una creciente desterritorialización de la violencia y una acentuada secularización de la agenda internacional. Así mismo, se ha cobrado una renovada trascendencia con la ingente actividad terrorista que pone en práctica el Estado Islámico en Medio Oriente y, sobre todo, en Europa” (Riquelme et al., 2019, s. p.).

Es importante tener presente que en el ambiente global aún persisten conflictos de carácter tradicional e interestatal, fenómenos que se analizan en los diversos dilemas de seguridad en Asia y Oriente Medio, como es el caso del inestable y complejo escenario de las dos Coreas; Japón y China; China y Rusia; Pakistán e India; India y China (Tokatlian, 2012). Asimismo, se pueden identificar en la compleja y crítica situación de conflicto actual entre Rusia y Ucrania, que comenzó en la mañana del 24 de febrero de 2022, cuando el presidente ruso, Vladimir Putin, ordenó a sus tropas bombardear e invadir el país vecino.

En este ambiente de interdependencia de los marcos regionales, se ha identificado que los actores estatales y no estatales tienen una serie de dificultades para enfrentar individualmente el amplio campo de demandas y desafíos que implica la globalización, especialmente en temas de seguridad. En este escenario, cabe recalcarlo, aparecen nuevas amenazas y adquieren relevancia las agrupaciones ilícitas transnacionales, la degradación del medioambiente y los desastres naturales, entre otros. En el caso de América Latina, la seguridad continúa siendo un tema prioritario para las sociedades y los gobiernos, de allí que en esta región se haya dado prioridad al estudio y análisis del crimen organizado transnacional (COT).

El crimen organizado transnacional en el orden mundial 2.0

El crimen organizado se involucra desde muchas perspectivas en las relaciones de la sociedad, relaciones que, sugerimos, se presentan entre los ciudadanos, el gobierno e inclusive traspasa fronteras, con efectos en términos de la seguridad. Como señala la Organización de Estados Americanos (OEA, 2003),

[...] el concepto de seguridad, que en un momento se enmarcaba principalmente en términos militares convencionales, hoy ha debido ampliar su marco de referencia y tener en cuenta una variedad de amenazas: terrorismo internacional, tráfico de drogas y armas ilegales, trata de personas, lavado de dinero, corrupción institucional y crimen organizado. En algunos países la pobreza, las enfermedades y la degradación del medioambiente contribuyen al deterioro de la seguridad humana. (p. 106)

Eso ocurre a través de la creación de un círculo vicioso que, como sugiere Cuervo (2018), establece redes de interdependencia capaces de socavar estructuralmente países y/o regiones (figura 1).

Figura 1. *El modus operandi de los ilícitos transnacionales.*



Fuente: Cuervo (2018).

Sin duda, la inestabilidad que el crimen organizado ha generado y continúa generando constituye una gran preocupación en el desarrollo de los procesos políticos, máxime cuando la sociedad concibe que el deterioro en la seguridad se debe única y exclusivamente a declives en temas económicos (Wielandt, 2007).

El accionar del crimen organizado no distingue entre sistemas políticos nacionales, entre actores y sus relaciones, mucho menos tiene en cuenta ni reconoce un sistema político internacional, en el cual la variedad de actores, la ausencia significativa de normas que regulen su relación, la marcada asimetría del poder y la transnacionalización de los límites de sus acciones tienden a acentuarse y pasan a ser indiscutibles. Para complementar esta conceptualización se debe mencionar que el orden mundial y sus actores, mecanismos y sistemas se pueden tornar de cierta forma abstractos si no se analizan desde una dinámica global ni se genera una construcción de análisis causalmente conjunto, de tal manera que cierre las brechas entre naciones que se involucran en el desarrollo de los ilícitos (Parrao, 2018).

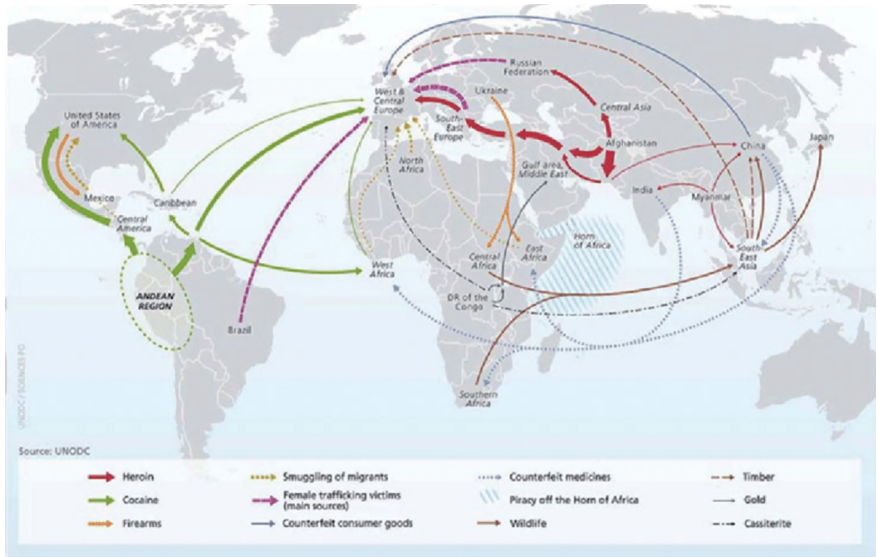
Por lo general, el crimen transnacional correlaciona organizaciones o individuos que se reúnen esporádicamente y que operan con mecanismos ciertamente

autorreguladores. En el artículo “Análisis de las organizaciones criminales transnacionales en la región”, Szeinfeld (2012) menciona que los objetivos de este tipo de amenazas consisten en obtener lucro monetario o comercial, por medios parciales o enteramente ilegales.

Por eso, William Werner (2009) clasifica el COT desde tres perspectivas: 1) política, que presenta al crimen organizado como resultado del debilitamiento de las estructuras estatales; 2) social, que destaca los elementos socioculturales como determinantes de la forma de actuar del COT; 3) económica, que explica el *modus operandi* desde la perspectiva de la demanda por bienes y servicios ilícitos.

Por su parte, el orden mundial 2.0 surgió desde finales de la última década del siglo XX, momento en el cual diferentes y nuevas ideas, nuevos elementos tecnológicos se insertan en la política, el comercio y la economía de todo el mundo. En ese escenario, una estructura más nueva del crimen organizado se configuró en el ciberespacio, un mercado electrónico en el que se venden bienes y servicios ilícitos y, en ocasiones, se infiltran negocios, sin contacto físico entre el proveedor y el cliente. A su vez, esa dinámica hace que el combate a las redes criminales sea una tarea más compleja, sobre todo en regiones como el espacio Andino-Amazónico, en el cual las conocidas debilidades estatales son amenazas para la estabilidad regional (figura 2).

Figura 2. Flujos de mercados del crimen organizado transnacional.



Fuente: United Nations Office on Drugs and Crime (2010, p. 2).

Por eso, es necesario que en el orden 2.0 las respuestas sean coordinadas e integradas entre las más diversas esferas de acción, en los niveles intra e inter estatales, para maximizar las capacidades de generar efectos duraderos en la búsqueda de: 1) modernizar los esfuerzos en el combate a la corrupción; 2) frenar las finanzas ilícitas; 3) fortalecer la arquitectura multilateral regional anticorrupción, y 4) mejorar los compromisos diplomáticos para cumplir los objetivos de la política anticorrupción, lo que será posible solamente por medio de una gobernanza intersectorial, como sugerimos abajo.

Estos eventos y muchos otros, que serán analizados posteriormente, han llevado a que los actores delincuenciales acojan este desarrollo y multipliquen su accionar, lo cual deja claro que la historia de la delincuencia, al igual que la de la política y la economía, ha evolucionado.

Teniendo en cuenta los desafíos que surgen del nuevo orden mundial, la reconfiguración de las amenazas y la perspectiva de que en Suramérica continúen los conflictos debido a la inestabilidad que causa el crimen organizado transnacional, es imperativo analizar cuáles actores son los que más están provocando estas amenazas, con el objeto de, en algún momento, identificarlos y desarrollar la mejor estrategia para contrarrestarlos.

Universo de investigación y la teoría de los Complejos Regionales de Seguridad

En el mundo contemporáneo, el tema de la seguridad internacional ha adquirido mayor importancia en el escenario global, no solo en el campo político, sino también en diferentes ambientes académicos que han propuesto que es necesario ampliarlo y profundizarlo para tornarlo más adecuado a las características de un orden sobre el cual aún existen muchas incertidumbres. En este contexto, se destaca la Escuela de Copenhague (Copenhagen Peace Research Institute [COPRI]), creada en 1985, que ha realizado una notable contribución al proponer la idea de *securitización*, que surge al ampliar el concepto de seguridad y con la premisa de que las amenazas no son solo militares, pues también pueden provenir de áreas políticas, ambientales, económicas y/o sociales, cada una con su propia dinámica.

Para los expertos de la Escuela, el nivel regional cuenta con mayor visibilidad en la medida en que, fuera del contexto de la rivalidad bipolar, los poderes locales ganaron mayor margen de maniobra y las peculiaridades regionales (especialmente

las preocupaciones de los Estados con los intereses y las intenciones de sus vecinos) se han tornado más fácilmente distinguibles de la agenda de seguridad sistémica de la Guerra Fría.

En ese sentido, otro aporte original e importante de esta Escuela es el modelo descriptivo de los Complejos Regionales de Seguridad (CRS). Su premisa básica, como se ha dicho, presupone que, en el mundo de la posguerra fría, las relaciones internacionales en el ámbito de la seguridad dan lugar a una mayor autonomía y relevancia a las dinámicas que ocurren en una escala regional.

La idea central es que existe un CRS cuando las principales percepciones y preocupaciones sobre la seguridad de los que forman parte de un espacio territorialmente coherente están tan interconectados, que dichos problemas no pueden ser razonablemente analizados o resueltos por separado. Según Buzan y Waever (2003), América del Sur encaja en este escenario y, para fines de esta investigación, también el arco Andino-Amazónico.

Así, los CRS son construcciones sociales derivadas de las relaciones de interdependencia que se establecen entre sus unidades a partir de interacciones entre variables materiales e ideaciones, tales como creencias, identidades, capacidades materiales, fronteras, distribución/percepción del poder y anarquía, las cuales dan al modelo mayor densidad analítica. En este marco conceptual, América del Sur tiene dos estructuras subregionales: el Subcomplejo de Seguridad del Cono Sur, formado por Argentina, Bolivia, Brasil, Chile, Paraguay y Uruguay, y el Subcomplejo de Seguridad del Norte Andino, que incluye a Perú, Ecuador, Colombia, Venezuela y Guyana, en el cual Brasil actúa, indirectamente, como un país de conexión entre los dos subcomplejos por su dimensión y por ser, al mismo tiempo, amazónico y andino.

El complejo Regional de Seguridad de América del Sur

América del Sur ha evolucionado en la integración del continente respecto a los temas de cooperación en seguridad con la creación de la Unión de Naciones Suramericanas (UNASUR), con la cual se conformó un bloque regional que abarca todos los países suramericanos. Entre las principales razones por las cuales se estableció se encuentran factores importantes, como el paulatino agotamiento de la efectividad y del consenso en torno al sistema interamericano actual y el fuerte debilitamiento de los ejes tradicionales de integración regional de América del Sur: la Comunidad Andina (CAN) y el Mercado Común del Sur (MERCOSUR) (Cujabante, 2012).

Es así como América del Sur buscó alternativas regionales multilaterales para combatir y atacar actores delincuenciales transnacionales y al mismo tiempo

fortalecer los lazos de unión y trabajo en conjunto entre naciones, como se había evidenciado en otros continentes. La UNASUR adquirió la imagen de un nuevo regionalismo, diferenciándose de los que en los años setenta habían emergido. En este sentido,

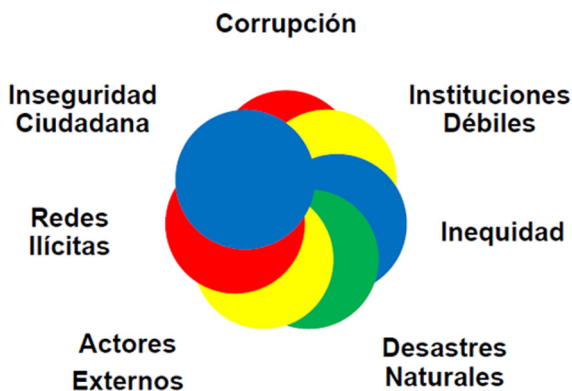
[...] el 8 de diciembre de 2004 se constituyó la Comunidad Sudamericana y a partir de la Cumbre de Isla Margarita, en abril de 2007, se le cambió el nombre por el actual, UNASUR, lo cual quedó protocolizado en el Tratado de Brasilia, firmado el 23 de mayo de 2008. (Cujabante, 2012, p. 70)

La UNASUR tiene un papel importante para la seguridad regional, como resulta evidente al revisar los actores que amenazan la seguridad y que están presentes en esta región geográfica después de la Guerra Fría. En este sentido, como se señaló en la definición del orden mundial 2.0, América del Sur está inmersa en un ambiente en el que los Estados ya no actúan solos y se constata el protagonismo de múltiples actores transnacionales. En respuesta a estos cambios globales, el análisis del concepto de seguridad ha evolucionado por lo menos en tres parámetros (Hurrell, 1998; citado por Cujabante, 2012):

[...] 1) el Estado ya no es el único objeto de referencia de la seguridad, sino que se deben incluir a los individuos y colectividades, a la humanidad en su conjunto, la gente en general, la biosfera, entre otros; 2) cualquier análisis significativo de la seguridad debe considerar la importancia de un rango de amenazas mucho más amplio, entre las que se incluyen aquellas cuyo origen se encuentra en la destrucción ambiental, en la vulnerabilidad económica y en la descomposición de la cohesión social y; 3) la responsabilidad de proveer seguridad radica no solo en el Estado, sino en instituciones internacionales y en organizaciones no gubernamentales. (p. 26)

Así las cosas, se comprende que dentro de los actores generadores de violencia e inestabilidad territorial comienzan a tener relevancia el terrorismo, el crimen organizado, las drogas, la corrupción, el tráfico de armas, la pobreza extrema, los desastres naturales, entre otros, que se destacan en lo que llamamos el Arco de Inestabilidad Andino-Amazónico. De esta manera, en la subregión se tiene una cadena de factores que crean un círculo vicioso integrado por las variables que se presentan en la figura 3.

Figura 3. *Círculo vicioso de amenazas andino-amazónicas.*



Fuente: Elaboración propia.

Por lo tanto, frente al tema específico de América del Sur, las amenazas que surgen se identifican y toman forma de acuerdo con las condiciones geográficas específicas, los recursos naturales que se producen, el ambiente político y, en ciertos casos, los procesos históricos, entre otros factores más. En síntesis, hay actores nuevos que están delinquiendo en zonas fronterizas y que transnacionalizan sus acciones, por ejemplo con las migraciones transnacionales por causa de la violencia y el comercio ilegal de armas, drogas, personas, recursos del medioambiente, etc.

El accionar de los grupos ilícitos en la triple frontera norte (Colombia, Brasil y Perú) –en lo que entendemos es uno de los ejes determinantes del Arco de Inestabilidad Andino-Amazónico– ha ido mutando, ya que en un principio solo intentaban demostrar un control local, pero en la medida en que han ido creciendo, primero demostraron ser fuertes y desarrollar un control territorial más ofensivo en las zonas del interior de estos Estados, y, posteriormente, ascendieron a un ambiente de transnacionalización delictiva con control de extensas zonas transfronterizas, como sucede en la actualidad.

Identificar estos grupos delictivos no era una tarea fácil porque el Estado no había mostrado interés en el tema, no era prioritario en sus políticas de gobierno y se pensaba que no representaban una amenaza para su estabilidad. Es así como el COT se encunó en zonas grises como el Trapecio Amazónico, donde hay espacios vacíos y olvidados por el Gobierno que les facilitan expandirse y alcanzar cierto poder. Con tal propósito, estas organizaciones criminales permean estructuras institucionales para controlar los pasos fronterizos y afianzar su control. Lo

cierto, como apuntaban Procópio (2007), Cuervo (2018) y Queiroz (2022), es que el espacio andino-amazónico ha ocupado cada vez más un papel destacado en el universo de cambios y cooperación entre los agentes del crimen organizado.

El Subcomplejo de Seguridad del Norte Andino

Si el Cono Sur optó por el camino de la integración y el fortalecimiento de la confianza mutua, el Subcomplejo de Seguridad del Norte Andino, a su vez, mantiene latentes las reminiscencias de un pasado de conflictos y rivalidades en un escenario agravado por problemas estructurales que trascienden los límites del Subcomplejo. Aún persisten los resentimientos derivados de las disputas territoriales de los siglos XIX y XX que involucraron a Perú, Bolivia, Chile, Venezuela, Colombia, Guyana y Ecuador (Buzan & Waever 2003).

Además, las serias debilidades político-institucionales que presenta el Subcomplejo constituyen un los principales factores responsables del vacío de poder que caracteriza la región, el cual ha sido ocupado por las redes del crimen organizado, responsables de la inserción de la subregión en el competitivo mercado ilícito mundial. Así, dadas las debilidades sistémicas comunes a los Estados andinos, el proceso de construcción estatal es una importante dimensión de la seguridad, componente esencial para el mantenimiento del orden regional en un contexto en el que la existencia de Estados débiles o fallidos cobra cada vez más un papel preponderante en la seguridad y la defensa.

Este cuadro de inestabilidad endémica también fue señalado por el Programa de Cooperación en Seguridad Regional (PCRS), que en un estudio lo identificó como uno de los graves problemas que enfrenta la región y que demanda especial atención, ya que "los Estados andinos han vivido [...] procesos de desinstitucionalización, corrupción gubernamental galopante, débil crecimiento económico, irracionalidad política, tendencias centrífugas e incluso debilitamiento de la viabilidad nacional" (Programa de Cooperación en Seguridad Regional PCRS & Fundación Friedrich Ebert, 2007, p. 3).

Como sucede en el contexto de Latinoamérica en general, en el CRS del Norte Andino y, por lo tanto, en el Arco Andino-Amazónico hay una fuerte actuación del crimen transnacional. El CRS es punto de producción, consumo y ruta de tránsito, lo cual ha contribuido al desarrollo de puntos estratégicos que utilizan las bandas criminales y que han favorecido su modo de actuar, de tal manera que no sean alcanzados por la vía legal.

Esto causa inestabilidad en los diferentes campos de acción de los Estados, como el político, militar, económico, ambiental y social. Al respecto, cabe mencionar el artículo de Meneses (2016) titulado “Crimen transnacional en América del sur y UNASUR”, en el cual trata los principales crímenes transnacionales y sus tipificaciones. Así mismo, presenta escenarios representativos con énfasis en los países de América del Sur, cuyo común denominador son las zonas grises y las fronteras extensas y con debilidades en seguridad y defensa.

Luego, como apuntan los investigadores, las amenazas y las vulnerabilidades que ocurren en el Arco Andino-Amazónico conforman una agenda compleja y difusa, marcada tanto por cuestiones transnacionales, vinculadas a la práctica endémica de actividades ilícitas, como por problemas endógenos derivados de las profundas debilidades estructurales que caracterizan a los países de la región (PCRS, 2006), algunos de ellos prototipos de Estados fallidos, en los cuales “las instituciones dejaron de funcionar o fueron regimentadas para servicios de intereses privados, muchas veces ilícitos” (Naím, 2005, p. 57).

Ilícitos transnacionales en el Subcomplejo de Seguridad del Norte Andino: ¿Un arco de inestabilidad basado en las redes del crimen organizado?

La seguridad en el Subcomplejo de Seguridad del Norte Andino es un tema prioritario para las sociedades y los gobiernos de los países de la Hilea Amazónica. Es un tema de estudio y preocupación debido al continuo desarrollo que presenta especialmente el COT, el cual se entiende como el ilícito que genera inestabilidad y está relacionado con “las ofensas cometidas en más de un Estado, así como aquellas ofensas que tienen lugar en un Estado, pero que son llevadas a cabo por grupos que operan en más de un Estado” (Riquelme et al., 2019, p. 10).

En la región se presenta un dinámico accionar de nuevos actores transnacionales relacionados con las extensas redes del COT. Así lo analiza Lucía Dammert (2012), quien señala que “en aquellos temas que tienen que ver con la seguridad pública, es decir, la percepción de la criminalidad, la ocurrencia de crímenes violentos, el fácil acceso a armas, las manifestaciones violentas y la evaluación de la policía, la región está marcada por la inseguridad” (p. 14). Así las cosas, la violencia

criminal se ha aposentado como uno de los más importantes desafíos a los gobiernos de la región.

En consecuencia, estos vínculos con las redes ilícitas internacionales y la cooptación interna en ciudades fronterizas, por ejemplo, permiten que se establezcan múltiples simbiosis entre las estructuras de la economía de contravención y la cultura del crimen organizado, en detrimento de la seguridad humana en las democracias amazónicas. Por esta razón, desde una perspectiva de seguridad pública el Subcomplejo de Seguridad del Norte Andino se distingue entre las zonas más violentas del mundo, lo cual determina uno de los desafíos más importantes que deben enfrentar las democracias latinoamericanas.

Estas preocupaciones se hacen evidentes al comprender que esta área geográfica presenta extensas zonas de porosidad de las fronteras, situación que sirve como combustible al crimen organizado, especialmente al vinculado con el narcotráfico, el tráfico de armas y a la trata de personas y al tráfico ilegal de inmigrantes, lo que también se encuentra en la base de ciertas tensiones bilaterales (Riquelme et al., 2019).

Murillo (2016; citado por Rodríguez & Nieto, 2020), visualiza y analiza el efecto que tienen los grupos de crimen organizado en las dinámicas políticas de los países de la región, pues se tiene evidencia de que la actividad ilícita ha influido directamente en el ejercicio del poder político. Este fenómeno se fortalece con la falta de gobernabilidad que se manifiesta en la fragilidad y debilidad de los diferentes Estados afectados, los cuales “han dejado de atender las necesidades de muchos sectores sociales y que estos grupos delictivos han aprovechado para ser legitimados por estos sectores de la sociedad” (Rodríguez & Nieto, 2020, p. 265).

Uno de los mayores ilícitos transnacionales en el Subcomplejo de Seguridad del Norte Andino es el tráfico de estupefacientes, razón por la cual este flagelo se debe considerar como la principal –todavía, claro, no la única– fuente de ingresos para este tipo de organizaciones y, en este sentido, se presume que quizás es la más importante amenaza a la seguridad, a los principios del Estado y a las relaciones de las naciones afectadas. Es importante resaltar que las consecuencias de las actividades que desarrollan estos grupos criminales afectan al ambiente, promueven la corrupción de las instituciones y causan un deterioro de la sociedad (Rodríguez & Nieto, 2020).

Al respecto, Tokatlian (2014) menciona que en un importante trabajo de Edwin H. Stier y Peter R. Richards de 1987 (“Strategic Decision Making in Organized Crime Control: The Need for a Broadened Perspective”) se encuentra una clara visión para

observar y evaluar cómo se despliega el crimen organizado a través de tres fases diferentes: predatorio, parasitario y simbiótico. En la primera fase, “predatoria”, el territorio y su control son fundamentales. El COT debe influir y tener el control de uno o varios bienes ilícitos en un espacio físico seguro; debe clarificar las rutas para el transporte de dichos bienes; tener acceso a mercados para realizar sus productos y proveerse de ámbitos de protección personal.

La segunda fase es la “parasitaria”: en este momento, la influencia política y económica del crimen aumenta notoriamente. Esta etapa no solo muestra la mayor inserción del crimen organizado, sino también tres dinámicas preocupantes: su legitimación, la proliferación y la democratización. El autor resalta que en esta fase es donde el crimen organizado muestra una importante corrupción de sectores públicos y privados. En la fase final, “simbiótica”, se evidencia el fortalecimiento de la criminalidad, al tiempo que el sistema político y económico se vuelve tan dependiente del crimen organizado como este de la estructura establecida. La frontera entre lo lícito y lo ilícito, entre lo legítimo y lo ilegítimo, se torna opaca y el Estado de Derecho mismo se diluye (Tokatlian, 2014).

De este análisis se infiere que en el Subcomplejo de Seguridad del Norte Andino, donde se observa un gran desarrollo del COT, se deben identificar estas etapas y analizar cada una de ellas para poder intervenir y desarrollar un conjunto de políticas y prácticas para frenar el crimen organizado, pues si no se hace de esta manera, la siguiente fase avanzará. Esto resulta clave para entender problemas como el del narcotráfico.

El Arco de Inestabilidad Andino-Amazónico: estudio de caso de la triple frontera norte entre Brasil-Colombia y Perú

Las premisas presentadas hasta este punto permiten inferir que, en lo que se refiere al Arco Andino-Amazónico, el narcotráfico internacional fluye por las débiles fronteras que caracterizan el orden mundial 2.0, lo cual evidencia que la fragilidad del Estado de Derecho es una causa importante, mientras que la escalada de violencia social local es una de sus consecuencias (Pinto & Rodríguez, 2020; Procópio, 2010; Queiroz, 2022). En cuanto al universo de análisis, como se verá más adelante, la triple frontera o Trapecio Amazónico –la región formada por las ciudades de Tabatinga (Brasil), Leticia (Colombia) y Santa Rosa de Javari (Perú)– se traduce en

un importante pasillo de distribución de ilícitos de variada naturaleza para las rutas de tráfico del mundo.

Sumado a lo anterior, es importante decir que la parte brasileña de la región representa una cercanía estratégica a las zonas productoras de droga ubicadas en Colombia y Perú, por lo que recibe la acción de los cárteles de la droga, principalmente colombianos, para movilizar su producción, con el objetivo de abastecer las rutas nacionales e internacionales por el río Solimões hasta Manaus y, de allí, a otras regiones del país y del mundo (Araújo, 2018).

La triple frontera norte entre Colombia, Brasil y Perú, por lo tanto, presenta un sinnúmero de problemáticas en relación con la lucha contra la ilegalidad, donde se encuentra el crimen organizado transnacional. En este sentido, resulta pertinente la idea de que, en esta área geográfica, el COT rompe las bases políticas y económicas de los Estados, “estimulando círculos viciosos de inseguridad, en la medida en que los integrantes de las redes criminales pueden colaborar con gobiernos corruptos, organizaciones paramilitares o grupos terroristas” (Gobierno de España, s. f., p. 1; citado en Rodríguez & Nieto, 2020, p. 266.).

Esta realidad conlleva la existencia de una población que vive, en general, con medios muchas veces insuficientes para cubrir sus necesidades básicas ante la fragilidad en las estructuras institucionales de la región, lo que llevó a Rebeca Steiman (2002) a calificar a la triple frontera norte como “periferia de la periferia”.

Esta es una zona en la que el COT, como hemos dicho reiteradas veces, emerge con inseguridad, malestar y deterioro en la sociedad, lo cual evidencia la convergencia de múltiples falencias institucionales. Es así como “el establecimiento permanente de actores armados ilegales en este espacio fronterizo se debe, en gran medida, a la ausencia y débil presencia del Estado colombiano en sus periferias” (Trejos, 2015, p. 1); pero no solo del Estado colombiano, sino también del Estado de Brasil y de Perú en esas tres principales “ciudades gemelas”: es decir, municipios divididos por una línea fronteriza entre países, que puede ser un río o el propio territorio, los cuales se encuentran estrechamente integrados en sus actividades cotidianas, sean económicas o culturales. Por todo eso, el alcance de esta interacción puede tener consecuencias prácticas para la soberanía de los Estados hacia sus territorios, situación agravada por la pujanza de un mercado financiero de drogas controlado por las redes del narcotráfico y que impacta fuertemente la vida financiera y social del Trapecio Amazónico (Steiman, 2002; Pinto & Rodríguez, 2020).

Así, se debe comprender que las dimensiones territoriales en la triple frontera norte dificultan la realización de las tareas del Estado para supervisar, dominar y

controlar tanto los flujos que traspasan sus fronteras, como los que se mueven de un punto al otro del territorio nacional. Esto abre el espacio para oportunismos, que se manifiestan en la degradación político-social de las instituciones en esa área que comprende 1.632 km² (figura 4).

Figura 4. Triple frontera norte Colombia, Perú y Brasil.



Fuente: Instituto Mayor Campesino (2015).

En complemento con lo anterior, Fernández (2016; citado por Sampó, 2018) señala que existe una verdadera red de grupos ilegales con calidad de logística y accionar, los cuales tienen efectos magnificados que nunca se habían evidenciado. Esto se debe a la gran capacidad de control y manejo que estos grupos tienen en la región, pero también a la falta de equipamiento y personal por parte de los Estados para asegurar el control efectivo de su soberanía.

El más importante y grande ilícito que acontece en la triple frontera, como sugieren los datos presentados, es el narcotráfico. Es un área donde existen y continúan en propagación redes internacionales de ilegalidad que se tejen en torno al narcotráfico, precisamente por la falta de presencia estatal y, ciertamente, de cumplimiento a la ley (Trejos, 2015). Es así como se considera que el Amazonas es de vital importancia para el narcotráfico debido a todas las vías fluviales con las que cuenta, ya que la mayoría desembocan en el río Amazonas en Brasil y de ahí salen al resto del mundo.

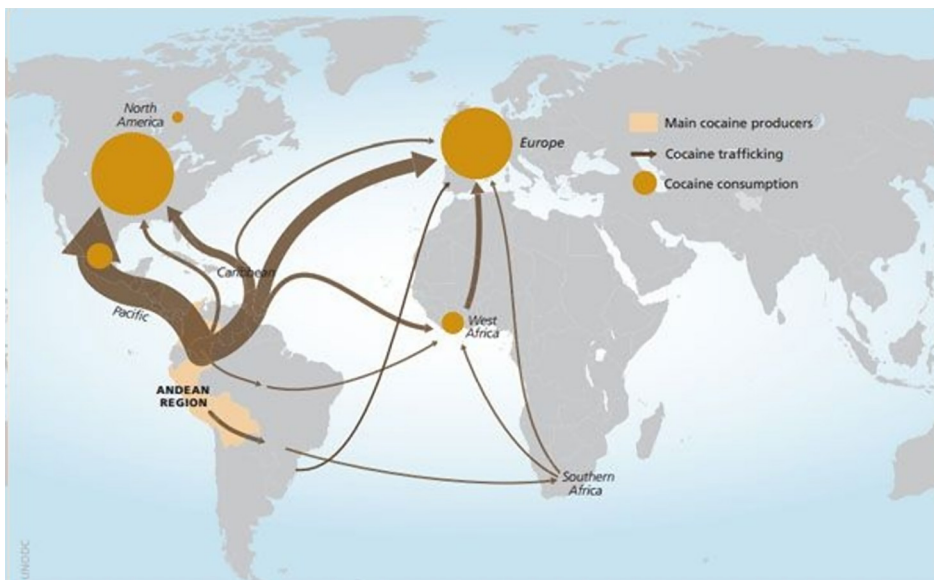
Como apuntan los datos del *Informe Mundial sobre Drogas* de la Oficina de las Naciones Unidas contra la Droga y el Delito (UNODC, por su sigla en inglés),

publicado en 2019, el mercado de la cocaína actúa como motor económico del Trapecio Amazónico, ya que Colombia y Perú son sus principales productores: juntos, los dos tuvieron un aumento del 78,8 % entre los años 2010 a 2017 (UNODC, 2019, p. 76). Además de destacar, nuevamente, que la ruta del río Solimões es una de sus principales salidas para la producción, asegura que Brasil se ha convertido en las últimas décadas en un gran mercado consumidor y no solo como una ruta de tránsito para el flujo de esta cocaína.

Como menciona Cuervo (2018), esto se debe a que el control en la zona fronteriza carece de instrumentos alternos y es insuficiente, puesto que entre los tres países no se dispone de la cooperación en seguridad necesaria para detener o disminuir las actividades ilícitas. Es preocupante que, a través de las carreteras, lanchas, avionetas y otros medios de transporte, se crucen libremente productos de contrabando.

Se confirma entonces que el espacio andino-amazónico, en la triple frontera norte, es un peligroso eje de inestabilidad que tiene un acelerado desarrollo en el contexto del orden mundial 2.0 (figura 5). Asimismo, también es reconocido como la ruta de escape de ilícitos –en especial de cocaína, que es un destacado producto amazónico con alto valor agregado–, lo cual constituye uno de los más urgentes desafíos para la construcción de una gobernanza en seguridad y defensa.

Figura 5. *Rutas de flujo de cocaína desde la triple frontera norte.*



Fuente: O Estado Net (2017).

Conclusiones

El orden mundial 2.0 es una realidad palpable y reconocible, como también lo son todas las externalidades generadas por las complejas relaciones de interdependencia, las cuales se presentan como posibles causantes de las inestabilidades regionales. En este sentido, si bien es un hecho que la globalización trajo innegables ventajas y facilidades en el intercambio de la información, así como en el incremento de las conexiones y espacios para el comercio, este escenario ha sido aprovechado por las redes del crimen para reproducir, por ejemplo, las cadenas delictivas de tráfico ilícito de armas, personas y drogas, principalmente (Pinto & Rodríguez, 2020). Por consiguiente, la economía ilegal se ha convertido en un problema que desborda la capacidad de los Estados del Complejo de Seguridad de América del Sur y se percibe como un reto compartido para ser enfrentado por todos.

Específicamente, este capítulo investigó el Subcomplejo de Seguridad del Norte Andino, en general, y más precisamente, lo que entendemos es un Arco de Inestabilidad Andino-Amazónico, el cual está en desarrollo para impulsar las redes del crimen organizado a partir de la triple frontera norte entre Brasil, Perú y Colombia.

Antes de proseguir en las conclusiones, es importante ponderar las limitaciones metodológicas de este estudio. Por una parte, la escasez de datos, sobre todo cuantitativos, no ha permitido establecer correlaciones plenas en cuanto a la hipótesis, y, por otra, las inferencias cualitativas recolectadas sugieren que existen causalidades entre las variables seleccionadas en la investigación: las dinámicas de inestabilidad en la triple frontera (variable dependiente), los niveles de fragilidad del Estado de Derecho y la geopolítica de las redes criminales que actúan en el Subcomplejo de Seguridad asociada a la economía de los ilícitos (variables independientes).

¿Entonces qué demuestran las inferencias descriptivas (cómo) y/o causales (por qué)? El incremento exponencial de las actividades ilícitas en esta región, compuestas y determinadas por el crimen organizado, ha hecho que el espacio de contacto entre Colombia, Perú y Brasil tenga repercusiones negativas en múltiples sectores, desde la economía hasta la seguridad y la defensa, lo cual ha generado ciclos viciosos de inestabilidades sistémicas.

De esta manera, es imperativo destacar la siguiente conclusión parcial: la dimensión que tiene el desarrollo del crimen transnacional bajo las peculiaridades locales en la triple frontera norte facilita el crecimiento de la economía ilegal. Dado que muchas personas buscan su sustento en la informalidad, existe el reconocimiento expreso y hasta la simpatía hacia aquellos que practican economías

illegales e informales, lo cual tiene implicaciones en las cadenas globales de los ilícitos hacia lugares de Asia, África y Europa, ya que el Arco Andino-Amazónico tiene una ubicación geográfica estratégica.

Entonces, confirmados los ilícitos transnacionales como factores directos en la generación de externalidades disruptivas, es importante reforzar la cooperación coordinada, policéntrica, entre países vecinos para atacar esta amenaza y desarticular cadenas de producción y consumo, de manera que se puedan contrarrestar las fuentes de inestabilidad que desafían, entre otros actores, a las Fuerzas Armadas.

Aunque el Estado de Derecho se encuentra en una situación de fragilidad, debido en parte a una economía que se basa cada vez más en las actividades ilícitas –como sugiere este estudio de caso–, se espera que los esfuerzos conjuntos sean capaces de propiciar la interacción de múltiples órganos de gobierno y de la sociedad civil para crear y hacer cumplir las reglas en ese dominio específico. En otras palabras, entendemos los mecanismos de gobernanza policéntrica como una de las mejores formas de lograr respuestas colectivas y eficientes ante las rupturas deletéreas causadas por las acciones del crimen organizado.

Finalmente, el análisis realizado permite sostener la hipótesis relacional directa de que “cuanto más transnacionales fueren las acciones de los ilícitos, mayor será la probabilidad de que el Subcomplejo de Seguridad del Norte Andino y, más específicamente, el espacio andino-amazónico, se convierta estructuralmente en un arco de inestabilidad basado en la fragilidad del Estado de Derecho y en la economía de los ilícitos”.

Referencias

- Araújo, T. (2018, 3 de octubre). Terra sem lei: Como abandono da Tríplice Fronteira amazônica ajuda o narcotráfico no país. *Sputniknews*. <https://tinyurl.com/yc3kz3pr>
- Aron, R. (1963). *Paz y guerra entre las naciones*. Revista de Occidente.
- Buzan, B., & Waeber, O. (2003). *Regions and powers: The structure of international security*. Cambridge University Press.
- Cuervo Ceballos, G. (2018). El crimen organizado transnacional como una amenaza híbrida para la Triple Frontera (Argentina, Paraguay y Brasil). *Revista Científica General José María Córdova*, 16(23), 43-61. <https://doi.org/10.21830/19006586.304>
- Cujabante Villamil, X. A. (2012). Unasur: ¿Hacia la consolidación de un complejo regional de seguridad? *Revista Científica de Estudios en Seguridad y Defensa*, 7(14), 78-16. <https://doi.org/10.25062/1900-8325.191>
- Dammert, L. (2012). *Seguridad ciudadana en el Perú: Las cifras del desconcierto*. Corporación Andina de Fomento.
- Haass, R. (2008). The age of nonpolarity: What will follow U.S. dominance. *Foreign Affairs*, 87(3), 44-56. <https://tinyurl.com/3mj4xz6b>
- Haass, R. (2017). World order 2.0: The case for sovereign obligation. *Foreign Affairs*, 96(1), 2-9. <https://tinyurl.com/mphmmfr2>
- Instituto Mayor Campesino (2015). *Migrantes forzados en la Amazonía: Una selva que refugia*. IMCA <https://tinyurl.com/z8rac2dw>
- Meneses Castillo, A. L. (2016). *Crimen transnacional en América del Sur y Unasur* [Tesis de maestría, Universidad Militar Nueva Granada]. Repositorio UNIMILITAR. <https://tinyurl.com/37beadt2>
- Naim, M. (2005). *Ilícito: Cómo el contrabando, los narcotraficantes y la piratería desafían la economía global*. Debate.
- O Estado Net. (2017, 1 de abril). O narcotráfico ameacador. <https://tinyurl.com/mzetx69j>
- Oficina de las Naciones Unidas contra la Droga y el Delito [UNODC]. (2019). Informe Mundial sobre las Drogas 2019. <https://tinyurl.com/yzjvhcem>
- Organización de Estados Americanos [OEA]. (2003). Conferencia Especial sobre Seguridad [Informe del Relator de la Conferencia Especial sobre Seguridad]. <https://tinyurl.com/4w5w6tff>
- Parrao, I. (2018). El orden mundial: Cuatro perspectivas teóricas y sus implicancias en el estudio de la realidad contemporánea. *Artigos Estratégicos*, 4(1), 33-44. <https://tinyurl.com/3n8y2tet>
- Pinto, E. M., & Rodríguez, D. (Eds.). (2020). *Crimen organizado transnacional: Fronteras y actores en el hemisferio*. Sello Editorial ESDEG; Planeta. <https://doi.org/10.25062/9789584288936>

- Procópio, A. (2007). *Subdesenvolvimento sustentável*. Juruá.
- Procópio, A. (2010). *Diplomacia e desigualdade*. Juruá.
- Programa de Cooperación en Seguridad Regional [PCRS] & Fundación Friedrich Ebert. (2007). *Integración, seguridad y conflictos en la subregión andina*. ILDIS-FES.
- Queiroz, F. (2013). Revisitando o conceito clássico de segurança: Dinâmicas, atores e validade analítica. *Intellector*, 9(19), 1-34. <https://tinyurl.com/msxu62uf>
- Queiroz, F. (2022). *La Organización del Tratado de Cooperación Amazónica (OTCA) como herramienta de combate al crimen organizado transnacional en el orden mundial 2.0*. William J. Perry Center for Hemispheric Defense Studies; National Defense University.
- Riquelme-Rivera, J., Salinas-Cañas, S., & Franco-Severino, P. (2019). El Crimen Organizado Transnacional (COT) en América del Sur: Respuestas regionales. *Estudios Internacionales*, 51(192), 9-33. <https://doi.org/10.5354/0719-3769.2019.52781>
- Rodríguez, A., & Nieto, E. (2020). Estrategia contra el crimen transnacional organizado en la triple frontera Brasil-Perú-Colombia desde la atención social integral de sus habitantes. En O. M. Ramírez-Villegas, H. Cancelado-Franco & N. R. Cárdenas-Rodríguez (Eds.), *Nuevas amenazas en el siglo XXI: Fronteras y Derechos Humanos* (261-298). Sello Editorial ESDEG. <https://doi.org/10.25062/9789584288950.09>
- Sampó, C. (2018). Brasil: La re-significación de la violencia como resultado del avance de organizaciones criminales. *Revista de Estudios en Seguridad Internacional*, 4(1), 127-146. <http://dx.doi.org/10.18847/1.7.8>
- Steiman, R. (2002). *A geografia das cidades de fronteira: Um estudo de caso de Tabatinga (Brasil) e Letícia (Colômbia)* [Tesis de maestría, Universidad Federal do Rio de Janeiro]. UFRJ. <https://tinyurl.com/25we5tdk>
- Szeinfeld, J. (2012). Análisis de las organizaciones criminales transnacionales en la región. *Revista do Laboratório de Estudos da Violência da UNESP/Marília*, (9), 58-68. <https://tinyurl.com/4rw6m4h4>
- Tokatlian, J. G. (2012). El entorno global. En K Derghougassian (Comp.), *La defensa en el siglo XXI: Argentina y la seguridad regional* (pp. 95-118). Capital Intelectual.
- Tokatlian, J. G. (2014, 11 de febrero). La Argentina y las etapas del narcotráfico. *La Nación*. <https://tinyurl.com/59jdwewy>
- Trejos, L. (2015). El lado colombiano de la frontera colombo-brasilera: Una aproximación desde la categoría de área sin ley. *Estudios Fronterizos*, 16(31), 39-64. <https://tinyurl.com/24wyd6ab>
- United Nations Office on Drugs and Crime (2010). La medición de los mercados y los flujos de productos. <https://tinyurl.com/mvjtnu44>
- Viola, E., Leis, & H. R. (2007). *Sistema internacional com hegemonia das democracias de mercado: Desafios de Brasil e Argentina*. Insular.
- Werner, G. C. (2009). *O Crime Organizado Transnacional e as redes criminosas: Presença e influência nas relações internacionais contemporâneas* [Tesis de Doctorado, Universidade de São Paulo]. Repositorio USP. <https://tinyurl.com/m4c5zut4>

Wielandt, G., & Artigas, C. (2007). *La corrupción y la impunidad en el marco del desarrollo en América Latina y el Caribe: Un enfoque centrado en derechos desde la perspectiva de las Naciones Unidas* [Serie Políticas Sociales, n.º 139]. Organización de las Naciones Unidas. <https://tinyurl.com/bded4ksp>

Zakaria, F. (2008). *The Post-American World*. W. W. Norton & Company.

Capítulo 11

Operaciones de Inteligencia y guerras en zonas gris^{*}

DOI: <https://doi.org/10.25062/9786287602809.11>

Oscar Fernando Rubio Ramírez
Jesús María Díaz Jaimes

Escuela Superior de Guerra "General Rafael Reyes Prieto"

Resumen: Este artículo trata sobre las Operaciones de Inteligencia y guerras en la zona gris, un tema reciente en los estudios estratégicos de las nuevas guerras. En primer lugar, se delimitan los conceptos y las características que le conciernen a los términos que se van a tratar. En segundo lugar, se enmarca el conflicto o la guerra en la zona gris –de carácter ambiguo y de difícil percepción–, la cual se desarrolla en muchos países y organizaciones criminales a nivel regional y mundial. Finalmente, en tercer lugar, se analizan los retos, oportunidades, alcances operacionales y estratégicos de la Inteligencia militar en escenarios contemporáneos de guerra y conflictos de zona gris. De esta forma se buscan estrategias que generen herramientas efectivas para desarrollar este tipo de conflictos en el escenario nacional e internacional.

Palabras clave: ambigüedad; conflicto; guerra híbrida; operaciones de inteligencia; zona gris.

^{*} Este capítulo es resultado de investigación adscrito al proyecto "*Naturaleza de la guerra contemporánea. Retos y oportunidades de las Fuerzas Especiales y la Inteligencia*", adscrito al Departamento Ejército de la Escuela Superior de Guerra, inscrito en la línea de investigación "Naturaleza de la guerra, terrorismo, nuevas amenazas", que forma parte del grupo de investigación Centro de Gravedad, con código COL0104976. Los puntos de vista pertenecen a los autores y no reflejan necesariamente los de las instituciones participantes.

Oscar Fernando Rubio Ramírez

Teniente Coronel del Ejército Nacional de Colombia. Magíster en Estrategia y Geopolítica, Escuela Superior de Guerra "General Rafael Reyes Prieto", Colombia. Diplomado en Oceanopolítica, Escuela Superior de Guerra del Ejército de Guerra Español. Profesional en Ciencias Militares, Escuela Militar de Cadetes "General José María Córdova", Colombia. Contacto: oscar.rubio@buzonejercito.mil.co

Jesús María Díaz Jaimes

Teniente Coronel (R) del Ejército Nacional de Colombia. Magíster en Estrategia y Geopolítica, Escuela Superior de Guerra "General Rafael Reyes Prieto", Colombia. Especialista en Ciencia Política, Universidad Autónoma de Bucaramanga, y en Gerencia, Universidad Militar Nueva Granada, Colombia.

<https://orcid.org/0000-0001-6595-8277> - Contacto: jesus.diaz@esdeg.edu.co

CitaciónAPA: RubioRamírez, O.F., & Díaz Jaimes, J. M. (2024). Operaciones de Inteligencia y guerras en zonas gris. En L. A. Montero Moncada & O. A. Garzón Gómez (Eds.), *Comandos: Retos de las Fuerzas Especiales e Inteligencia en la guerra contemporánea* (pp. 257-286). Sello Editorial ESDEG. <https://doi.org/10.25062/9786287602809.11>

COMANDOS: RETOS DE LAS FUERZAS ESPECIALES E INTELIGENCIA EN LA GUERRA CONTEMPORÁNEA

ISBN impreso: 978-628-7602-79-3

ISBN digital: 978-628-7602-80-9

DOI: <https://doi.org/10.25062/9786287602809>

Colección Seguridad y Defensa

Sello Editorial ESDEG

Escuela Superior de Guerra "General Rafael Reyes Prieto"

Bogotá D.C., Colombia

2024



Introducción

Los conflictos armados o guerras mundiales, en especial los llevados a cabo a finales del siglo XIV hasta nuestros días, han pasado por múltiples cambios en el campo de batalla. Empezando con la guerra de primera generación, que incluye las guerras europeas que libraron los ejércitos napoleónicos en el siglo XIX con el fin de conquistar o asegurar la soberanía de territorios, su característica principal fue el uso en masa de las armas de fuego en el campo de batalla hasta el siglo XX (Aznar, 2015). El uso de grandes cuerpos de ejércitos que se enfrentaban de forma directa fue aplicado en la Primera Guerra Mundial, la cual sirvió para evolucionar a nuevos conceptos, como la guerra indirecta del pensador militar Liddle Hart, quien inspiró la guerra móvil o relámpago (*blitzkrieg*) del ejército alemán en la Segunda Guerra Mundial (Del Rey & Canales, 2012). Las características más importantes de este tipo de guerra son la industrialización y la mecanización, siendo uno de sus elementos fundamentales la capacidad de movilizar grandes ejércitos y el uso de maquinaria bélica, lo cual generó nuevas tecnologías para la creación de armas y doctrinas para aplicarlas.

Asimismo, a partir de Carta de las Naciones Unidas del 26 de junio de 1945 y de los Convenios de Ginebra del 12 de agosto de 1949 (que introducen el concepto eminentemente material de *conflicto armado*), se generaron nuevas reglas y deberes que los Estados deben cumplir en caso de un conflicto entre Estados o dentro de ellos, según sea el caso (Raggio, 2019). Estas normativas marcaron los múltiples conflictos de la segunda mitad del siglo XX, en lo que se conoció como la Guerra Fría, en el cual participaron las dos superpotencias hegemónicas del momento: por un lado, la Unión de República Socialistas Soviéticas (URSS), que encarnaba el modelo comunista de desarrollo, y, por el otro, los Estados Unidos de América (EE. UU.), que lideraba el modelo capitalista-liberal. Aunque la principal

característica de este conflicto fue que no hubo confrontación armada directa entre las fuerzas militares, estas sí participaron activamente en la ampliación de sus espacios de influencia en terceros países de todos los continentes para debilitar el dominio político, económico o militar de su adversario.

Esta situación dio como resultado la intensificación de muchos conflictos internos en muchos países, entre otros en Vietnam, Nicaragua, Laos, Afganistán y el Congo, en los cuales se armaron y entrenaron muchos grupos irregulares para que tomaran el poder del Estado que confrontaban. En este escenario surgió el concepto de *guerra asimétrica*, el cual se refiere al uso de métodos no convencionales, tales como el terrorismo, la guerra política, la guerra sucia, la contrainsurgencia y la desinformación (Cuneo, 2019), pues la disparidad en la fuerza militar para atacar se compensaba con estos métodos para cumplir los objetivos políticos. Dado que estas condiciones forjaron un nuevo tipo de guerra muy difícil de afrontar por parte de los Estados en el marco del Derecho Internacional Humanitario (DIH), se violaron muchos Derechos Humanos y se crearon o consolidaron varias dictaduras de diferente corte en el mundo durante la Guerra Fría.

Cuando la URSS colapsó en 1991 ante el fracaso de su modelo económico y político, se desencadenó la desintegración de los Estados que la conformaban, en especial los del este de Europa, y la pérdida de su área de injerencia en varias partes del mundo. Esto dio paso a una nueva era de conflictos internos y al auge de grupos radicales religiosos musulmanes, los cuales generaron la mayor acción terrorista a comienzos del siglo XXI: impactaron dos aviones comerciales en las Torres Gemelas en la ciudad de New York. Este ataque tuvo como resultado una nueva guerra, esta vez contra el terrorismo, que fue liderada por el gobierno Bush (Correa, 2017).

Como represalia, el gobierno de los Estados Unidos intervino directamente en varios países para atacar a las células militares de los grupos armados que utilizan el terrorismo islámico, denominados yihadistas; este es el caso de Al Qaeda, que tenía su base de entrenamiento en Afganistán o en Iraq para derrocar al dictador Sadam Husein. Estas guerras dieron como resultado un incremento considerable en la afectación a la población civil debido al uso indiscriminado de acciones terroristas, como vehículos bomba y ataques suicidas, tácticas difíciles de contrarrestar por un ejército regular.

Como consecuencia de la caótica situación de seguridad y debido a la proliferación de múltiples grupos irregulares en Iraq, después de la invasión de los Estados Unidos surgió en 2014 el grupo yihadista Daesh, el autodenominado

Estado Islámico o también conocido como ISIS o ISIL, que profesan la rama más tradicional y ortodoxa del islam, la suni, grupo que desplazó de la escena a Al Qaeda y Al Nusra (Muñoz, 2018). Esto generó una confrontación directa contra los ejércitos iraquí y sirio, la cual resultó en la apropiación de bastas áreas de cada país y en la proclamación de un nuevo califato.

Las consecuencias de estos hechos desembocaron en una guerra regional de gran escala en la península arábiga, en la cual el uso de los medios de comunicación y las redes sociales adquirieron un nuevo papel, pues estas herramientas fueron indispensables en el reclutamiento y la expansión de su ideología en todo el mundo. Como resultado se produjeron múltiples ataques terroristas en Europa y los Estados Unidos por parte de los denominados *lobos solitarios* (Cuneo, 2019), que son personas reclutadas por medio de redes sociales para ejecutar ataques terroristas de resonancia y así posicionar el grupo en la escena mundial. Sin embargo, gracias a la campaña militar que realizaron las fuerzas de la Organización del Tratado del Atlántico Norte (OTAN), Rusia e Irán, las cuales apoyaron a las autoridades locales de Iraq y Siria con ayuda militar y financiera, se logró en 2017 derrotar militarmente a Daesh, de tal manera que estas fuerzas pudieron mantener sus intereses estratégicos en la región.

Ahora bien, respecto al entorno regional del continente americano, se debe señalar que en sus hemisferios centro y sur existen grupos armados que utilizan métodos y acciones de carácter terrorista para cumplir sus fines, como sucede en México con los Zetas o el cartel de Sinaloa. Dichos grupos narcotraficantes cuentan con un gran poder económico que obtuvieron con el tráfico de estupefacientes, han construido grandes ejércitos con arsenal militar proveniente de los Estados Unidos y tienen un control total en algunos Estados donde son ley.

Por medio de la intimidación y los asesinatos selectivos, estos grupos logran efectuar cogobierno y participan activamente en el desarrollo de las políticas regionales (Zavala, 2018) para cumplir sus propios intereses. Frente a esta situación, el Estado mexicano, en cabeza de sus Fuerzas Armadas, ha dado una lucha frontal contra estas organizaciones y ha fortalecido su capacidad operativa y de inteligencia, lo cual dio como resultado en el año 2016 la captura del líder del cartel de Sinaloa conocido con el alias del *Chapo Guzmán*.

Respecto a Colombia, se identifican varios grupos armados, algunos con más de cincuenta años de existencia, como es el caso del Ejército de Liberación Nacional (ELN). Otros grupos se formaron a partir de las desmovilizaciones de antiguas agrupaciones armadas, por ejemplo el Clan del Golfo, que absorbió a

algunos antiguos integrantes de las Autodefensas Unidas de Colombia (AUC) y sus áreas de injerencia (Bolaños, 2018). Otro ejemplo tuvo lugar con el proceso de paz entre el Gobierno colombiano y las Fuerzas Armadas Revolucionarias de Colombia (FARC), que derivó en el surgimiento de varias facciones o grupos, como las FARC Residual, La Segunda Marquetalia y los Comandos de Frontera.

En este escenario, las Operaciones de Inteligencia han sido la punta de lanza de todos los organismos de inteligencia del Estado para dismantelar dichas organizaciones, donde el ingenio y el uso del engaño son importantes. A modo de ejemplo, se puede mencionar la operación “Jaqué”, desarrollada el 2 de julio del 2018, en la que los miembros de la Inteligencia militar usaron una fachada e historia ficticias para hacerse pasar por una organización no gubernamental (ONG) que, aparentemente, recogería a quince secuestrados que tenían las FARC, entre ellos la excandidata presidencial Ingrid Betancourt, secuestrada desde 2002 (Bolaños, 2018). Estas personas fueron liberadas después de que abordaran un helicóptero que, supuestamente, los llevaría adonde se encontraba Guillermo León Sáenz Vargas, alias *Alfonso Cano*, cabecilla principal de la organización en esa época. Durante esta operación fueron capturados dos cabecillas del Frente Primero, Gerardo Aguilar, alias *César*, y Alexander Farfán, alias *Enrique Gafas*, sin efectuar disparo alguno.

Cabe señalar que esta Operación de Inteligencia es un referente mundial del modo como se pueden obtener resultados operacionales estratégicos y de alto impacto nacional sin recurrir al uso de armas de fuego. La principal lección es que el conocimiento y el análisis de la manera como opera o delinque una organización, grupo criminal o fuerza enemiga que se quiere atacar, permite bloquear sus fortalezas y explotar al máximo las debilidades para conseguir los objetivos que se persiguen.

Debido a esto, las Fuerzas Militares y de Policía colombianas han pasado por un proceso de transformación en su capacitación y doctrina para contrarrestar las múltiples amenazas que enfrentan. En este contexto, las Operaciones de Inteligencia se refieren a las tareas que realizan las unidades de Inteligencia militar y unidades de combate para obtener información que contenga las respuestas sobre los requerimientos críticos del comandante (Schachtner, 2018). Específicamente, el personal de la especialidad de Inteligencia es el encargado de planear y ejecutar las Operaciones de Inteligencia contra las amenazas y grupos armados que delinquen en sus áreas de operaciones.

En resumen, la guerra se ha transformado acorde con el desarrollo humano en un mundo globalizado. La naturaleza de los conflictos ha experimentado muchos cambios, especialmente al final de la Guerra Fría, de manera que no es común observar conflictos entre ejércitos de Estados-naciones, con la excepción de la guerra actual entre Rusia y Ucrania, ya que las confrontaciones armadas se han enfocado en guerras internas o civiles, así como en la creación de grupos radicales que buscan cumplir sus objetivos o fines políticos por medio de métodos no convencionales, entre los cuales se encuentra el terrorismo. Estas características generan un espectro no físico llamado la *zona gris*.

En este espectro de guerra en zona gris prevalecen las acciones políticas, económicas, jurídicas, convencionales y no convencionales que, a la postre, buscan socavar el ímpetu o deseo de confrontación del adversario para que cumpla con los deseos u objetivos del Estado. En este contexto, lo más importante es que no se comprometa de forma directa el actuar de las fuerzas regulares de la nación, que es lo que llevaría a escalar en una tensión diplomática o, en el peor de los escenarios, una confrontación bélica.

Conceptos “Operación de Inteligencia” y “zona gris” dentro del desarrollo de las guerras contemporáneas

Operación de Inteligencia

La inteligencia, según la definición de la OTAN, en un sentido amplio y dentro del contexto militar, es el resultado de la integración e interpretación de nuestros conocimientos sobre el terreno, la meteorología, las actividades, las capacidades y/o las intenciones de un enemigo actual o potencial (Sainz, 1991). Tiene la intención de comprender o entender el comportamiento de la amenaza para obtener un conocimiento amplio y profundo del modo como actúa o delinque. También se considera como una disciplina que sigue un proceso lógico, una secuencia de pasos que conducen a un producto o una información final que pueda servir al mando operacional para la toma de decisiones.

En este sentido, una Operación de Inteligencia incluye las tareas o acciones efectuadas por personal capacitado y entrenado en recolectar información del enemigo o amenaza, la cual varía según la doctrina militar del país (Quiñónez, 2012).

Normalmente, los conceptos se desarrollan con base en las experiencias que haya tenido en las diferentes guerras en que esté inmerso y en el tipo de guerra, ya sea convencional o irregular/no convencional. Vale la pena mencionar que estas actividades son planeadas y ejecutadas por personal entrenado y capacitado para dichas misiones, quienes son conocidos como agentes de inteligencia y que deben cumplir unos requisitos y condiciones especiales para cumplir estas tareas, que son designadas por las autoridades pertinentes de un Estado o nación.

Los agentes de inteligencia cuentan con un perfil definido, así como con unas características físicas y psicológicas que se adaptan al entorno o las circunstancias en las que se desea operar. Estos agentes deben ser capaces de efectuar el ciclo de inteligencia, especialmente en el planeamiento y la recolección de información, para así generar un análisis y uso de la información de forma óptima y de acuerdo con los objetivos y alcances que se desean en la Operación de Inteligencia. La mayoría de los agentes secretos son hombres callados y muy discretos, capaces de infiltrar sin mayor sospecha altos círculos diplomáticos, gubernamentales o empresariales (Swenson & Sancho, 2015), pues se saben mimetizar utilizando hábilmente una fachada o historia ficticia que les facilita y genera una seguridad para no ser descubiertos por el enemigo.

Asimismo, existen al menos tres grandes necesidades que se cubren con los diferentes tipos de inteligencia: la inteligencia militar, la inteligencia estratégica y la información policial o criminal (Swenson & Sancho, 2015). Según el caso, los agentes efectúan actividades u Operaciones de Inteligencia para prevenir, detectar y neutralizar amenazas o delitos que existen en el entorno de seguridad y defensa de un país, los cuales pueden cambiar en función de los intereses nacionales y geopolíticos que enfrentan en cualquiera de los dominios, ya sea de carácter terrestre, marítimo, aéreo, cibernético, logístico o biológico (Méndez et al., 2019).

En este contexto, las Operaciones de Inteligencia se desarrollan de acuerdo con las necesidades o vacíos de información que requiere el mando para planear sus operaciones. Como se detalla en los siguientes apartados, las Operaciones de Inteligencia se clasifican de en espionaje, sabotaje, decepción, psicológicas, información y neutralización.

Espionaje

Es la tarea principal de cualquier agencia de inteligencia desde la concepción de los antiguos Estados, los cuales la efectuaban para recopilar información de las capacidades y debilidades de los Estados rivales y, a partir de allí, planear sus ataques.

El espionaje es una actividad encubierta que se realiza para obtener información clasificada mediante el empleo de espías, para beneficio de una organización o de un Estado, por lo cual el espía debe ser un individuo de gran preparación y altamente adiestrado para obtener información clasificada de carácter político, económico, psicosocial o militar utilizando procedimientos clandestinos o encubiertos (Llop et al., 2013).

Según Gamboa (2016), el viejo concepto de *inteligencia/espionaje*, que se centraba en las meras tareas informativas sobre “lo secreto”, hace tiempo que fue superado para dar paso a otro de horizonte mucho más abierto y que exige una mayor integración con el objetivo de realizar nuevas y complejas tareas, desarrollarlas con fundamento científico y adaptarlas a la obtención y tratamiento de la información procedente de nuevos y numerosos ámbitos (Gamboa, 2016).

Asimismo, de acuerdo con sus necesidades y la misión asignada, el espionaje explota diferentes fuentes de información, como el reclutamiento de personas que tengan acceso a información, la documentación de interés, la transmisión técnica de información, las actividades propias del agente o espía, la infraestructura física para efectuar las actividades de inteligencia, el material o el equipo y el ambiente natural, que es el estudio del entorno físico donde se ejecutan las actividades de espionaje (Llop et al., 2013).

Con la globalización de la información por medio del internet, es muy fácil acceder a múltiples “fuentes abiertas” (OSINT, por la sigla en inglés de Open Source INTElligence), las cuales proporcionan grandes volúmenes de datos que son difíciles de seleccionar, contrastar y analizar adecuadamente. Por ello se hace necesario el uso amplio de las nuevas tecnologías que puedan ayudar en la búsqueda y el rastreo de información de interés nacional.

Las agencias de inteligencia avanzadas del mundo se han adaptado al nuevo escenario internacional globalizado y aprovechan ahora las posibilidades que ofrecen las tecnologías de la información y la comunicación (TIC). Finalmente, cabe señalar que las agresiones por parte de Estados, grupos o individuos con la finalidad de lograr información que les permita obtener ventajas estratégicas, políticas o económicas, han sido una constante histórica y siguen siendo una amenaza de primer orden para la seguridad (Gamboa, 2016).

Sabotaje

También conocida como *subversión*, es el conjunto de acciones encubiertas de violencia física realizada contra los bienes materiales, sean estos de propiedad

individual, colectiva o pública; estas acciones van desde la simple alteración de la función que cumple hasta su destrucción total (Llop et al., 2013). En un contexto general, la finalidad del sabotaje es desestabilizar al Estado en cualquiera de sus ámbitos, bien sea económico, político, social o militar, para obtener ventajas tácticas que a la postre tendrían consecuencias estratégicas a favor.

Esta actividad va ligada a la ejecución de operaciones militares que, en una guerra convencional, buscan cumplir los objetivos que el Estado ha definido contra la amenaza o enemigo; es decir, a diferencia de la guerra no convencional, no necesariamente se realizan operaciones militares para afectar al enemigo y cumplir los objetivos. La ejecución de cualquier acción de sabotaje requiere de informaciones para tener un conocimiento de las características específicas y técnicas del objetivo por sabotear, de manera que el enemigo o adversario externo o interno orientará sus esfuerzos para satisfacer estas necesidades de información (Llop et al., 2013).

Los objetivos que se pueden cumplir con el sabotaje dependen de la capacidad del Estado u organización en acceder a los bienes materiales o redes informáticas del enemigo, pues de esto depende que tenga las condiciones para afectar la documentación importante, la infraestructura crítica, el material y el equipo de las fuerzas armadas enemigas, la infraestructura informática o páginas web de las instituciones gubernamentales, y el ambiente natural o geográfico que puedan generar una ventaja táctica o estratégica (Llop et al., 2013). Con este propósito se utiliza la modalidad de sabotaje incendiario, es decir, el sabotaje con explosivos utilizado especialmente contra infraestructura crítica; el sabotaje mecánico contra los equipos y las capacidades militares enemigas, y, el más utilizado en la actualidad, el sabotaje informático para robar información, impedir o neutralizar el funcionamiento de los sistemas informáticos de la amenaza.

Decepción

Las operaciones de decepción se usan para efectuar un engaño militar o desinformación, que según Andrade et al. (2011) son las acciones ejecutadas con el objetivo de engañar a los adversarios sobre las capacidades, intenciones y operaciones de las fuerzas militares propias, promoviendo un análisis equivocado y causando que el adversario obtenga conclusiones falsas. De esta manera se búsqueda obtener una ventaja en las operaciones militares o de inteligencia y minimizar los efectos adversos de las acciones enemigas sobre los intereses nacionales.

Además, otro objetivo de las operaciones de decepción es erosionar la credibilidad de las personas u organizaciones adversarias en su toma de decisiones

manipulando su percepción de realidad. Con ello se busca ganar tiempo y resquebrajar la unidad de mando militar o la política del adversario, pero sin comprometer una gran cantidad de tropas o equipos militares para obtener ventajas estratégicas. En el ámbito de las Operaciones de Inteligencia, este tipo de operaciones de decepción se aplica en el campo de la inteligencia humana y técnica, así como en las comunicaciones enemigas y en su estructura informática.

Psicológicas

Hacen referencia a la estrategia planeada y dirigida para utilizar un conjunto de elementos, como la propaganda, los medios de comunicación y otras formas de acción psicológica –empleados por cualquiera de las fuerzas en conflicto–, con el propósito de influir en la voluntad, la actitud y el comportamiento de las tropas, los grupos de población y los miembros de las organizaciones hostiles (Andrade et al., 2011) para buscar ventajas estratégicas y lograr el éxito en el desarrollo de la guerra.

Dado que las operaciones psicológicas están encaminadas a brindar apoyo a las operaciones militares, no pueden ser ejecutadas por fuerzas independientes. Específicamente, se dividen en tres categorías: de carácter estratégico, táctico y de consolidación, dependiendo de las características geográficas del ambiente operacional, el blanco audiencia que se quiere impactar y el tiempo estimado para su ejecución. Por ende, las operaciones psicológicas de consolidación se desarrollan en áreas en las cuales ya existe control por parte del Estado, que busca generar una normalidad y apoyo de la población civil.

En este sentido, se hace necesario el uso de tecnología de vanguardia con capacidad de penetrar los medios de comunicación enemigos, bien sea de forma directa o indirecta, para generar la matriz de opinión o percepción de acuerdo con los objetivos establecidos y obligando al adversario a pelear en nuestro campo de información o desinformación, lo cual daría un resultado en el campo táctico o estratégico positivo según los objetivos planteados para la misión.

Asimismo, existen numerosos métodos que se pueden emplear en las operaciones psicológicas, dependiendo de los múltiples factores y las categorías que se utilicen, como los sistemas de transmisión de radio y televisión; la distribución por aire de material impreso o panfletos, obsequios y otros útiles; campañas de rumores contra el adversario; publicar derrotas militares enemigas; escasez de alimentos, falta de alojamiento, ropa o cualquiera de los artículos de primera necesidad; fraccionamiento y falta de confianza interna; conflictos por la administración y manejo de recursos económicos (Andrade et al., 2011), y, en general, cualquier debilidad en el sistema enemigo que ayude a diezmar su voluntad de lucha.

Información

Son las actividades de Inteligencia encaminadas a usar la información para cumplir los objetivos nacionales. Como la diplomacia, la competencia económica o el uso de la fuerza militar, la información por sí misma es un aspecto esencial del poder nacional (Andrade et al., 2011); en todo caso, estas pueden ser utilizadas de forma simultánea en operaciones defensivas y ofensivas para cumplir con la misión, así como para proteger las capacidades propias y atacar sistemáticamente a la amenaza.

Para ello se utilizan todos los medios de difusión de información con los que se cuentan: radio, televisión, medios escritos, redes sociales y medios digitales. Además, se debe cumplir con unos criterios de calidad de la información que están relacionados con la exactitud, la relevancia, el sentido del tiempo, el valor práctico, la información completa, la brevedad y la seguridad, con el fin de obtener un producto informático óptimo para usarlo con el blanco audiencia que se quiere desinformar o fortalecer, según sea el caso.

Los objetivos de las operaciones de información son amplios y de gran alcance, ya que actualmente la sociedad se encuentra hiperconectada por los medios digitales y las redes sociales. Por ende, los agentes de inteligencia deben estudiar y planificar para influir exitosamente sobre el blanco audiencia elegido, explotando sus emociones, motivos y razonamiento objetivo, así como el comportamiento de sus gobiernos, organizaciones, grupos e individuos (Andrade et al., 2011), con el fin de destruir, interrumpir o negar el uso de la información del adversario, además de degradar, engañar, explotar, influir, proteger, detectar, restaurar o responder cualquier información enemiga que afecte la credibilidad de las instituciones, personas u organizaciones propias.

Neutralización

Las operaciones de neutralización son aquellas que van encaminadas a anticipar cualquier acción bélica o no armada que pueda afectar la integridad o las instituciones de un Estado u organización. De esta manera, se busca contrarrestar las intenciones, amenazas y objetivos de los adversarios o enemigos mediante la “contrainteligencia” (Quiñónez, 2012), para afectar la capacidad de mando y control del adversario, por ejemplo, liquidando los comandantes de las unidades enemigas con métodos no convencionales u operaciones militares con unidades de Fuerzas Especiales.

También se busca afectar la capacidad logística o económica de la amenaza atacando su infraestructura crítica y, sobre todo, las figuras políticas o militares

enemigas beligerantes. Como ejemplo se puede mencionar la operación que realizaron los Estados Unidos en el año 2020 para matar al general iraní Qasem Soleimani, comandante en jefe de las fuerzas Quods en Irak, quien era visto como una posible amenaza a la seguridad o legitimidad de dicha nación.

De esta manera, se concluye que las Operaciones de Inteligencia no solo deben dirigirse contra las amenazas directas, pues si bien el espionaje proporciona las informaciones o insumos necesarios para prevenir, detectar y neutralizar una amenaza, también da los argumentos necesarios para efectuar planeamiento prospectivo sobre los posibles cambios en el ámbito político, económico, militar o social que puedan afectar los intereses nacionales o estratégicos del Estado.

Zona gris

El concepto de zona gris fue acuñado recientemente por académicos en geopolítica y desarrollado por algunos Estados, que lo definen como un espectro o un nuevo teatro de la guerra no convencional, de carácter ambiguo, que no cuenta con un espacio físico definido. Sin embargo, se debe señalar que algunos actores no reconocen esta zona ni la delimitan en el análisis estratégico que hacen sobre su seguridad, pues dado que su estrategia cuenta con varias dimensiones y aristas, se dificulta que creen una estrategia general rígida. Además, si la pusieran en práctica, no generará en algunos casos el objetivo final en corto tiempo (Jordán, 2018), de manera que los métodos y las técnicas para poder atacar los diferentes elementos que existen en la zona gris se deben generar de forma gradual y concisa.

Características de la zona gris

La zona gris hace referencia a un concepto amplio y con unas características difíciles de percibir a primera vista, pero que las naciones y las organizaciones criminales desarrollan para cumplir sus objetivos estratégicos. Específicamente, este espectro cuenta con cuatro características: ambigüedad, gradualismo, intereses sustanciales en juego y estrategias multidimensionales, las cuales se describen en los siguientes apartados.

Ambigüedad

Se refiere a que no se plantean relaciones pacíficas ni conflicto armado. En el conflicto en la zona gris, la competición estratégica entre dos o más Estados (con sus respectivas diadas conflictivas) discurre por debajo del umbral de violencia política del conflicto armado menor (Baqués, 2017). Es decir, una confrontación a pequeña

escala, donde pueden existir reclamos verbales, protestas y utilización de la población civil en contra de las autoridades, lo cual puede generar una disputa política a lo largo del tiempo.

En esta característica también tienen un papel las Fuerzas Militares, que pueden efectuar ejercicios disuasorios o de demostración de fuerza en las áreas de confrontación o en las fronteras entre naciones, pero evitando que se escale a un conflicto armado abierto. A modo de ejemplo vale la pena mencionar el envío de aviones de combate de la Fuerza del Aire de la República Popular de China sobre las aguas territoriales de Taiwán; este caso muestra que se procura no cruzar líneas rojas que puedan desembocar en una contienda militar con costes muy elevados y consecuencias imprevisibles (Mazarr, 2015). En este sentido, para el Estado más fuerte tiene un papel importante conocer la capacidad de respuesta de su adversario para evitar una contestación de carácter bélico más fuerte y amplia, la cual se puede tornar en una guerra directa que salga del espectro de la zona gris.

Esta ambigüedad intencionada dificulta tanto la identificación de las actividades hostiles propias de la zona gris, como la articulación de estrategias de respuesta (Mazarr, 2015). Por esta razón, para las agencias de Inteligencia y la estrategia general es importante saber los objetivos políticos que persigue la amenaza y los medios con los que cuenta para atacar en la zona gris, de manera que pueda prevenir, detectar y, en lo posible, neutralizar las intenciones o disminuir las consecuencias de las acciones enemigas.

Gradualismo

El gradualismo refuerza la ambigüedad, pues la gravedad última y la interrelación de las distintas acciones no siempre resultan obvias a los decisores políticos del rival, a sus aliados ni a sus respectivas opiniones públicas (Mazarr, 2015), en un contexto en el que el tiempo no puede ser definido y los resultados o progresos que se quieren lograr suceden de forma lenta o paulatina. Además, esa gradualidad hace que se establezca un *statu quo* en las acciones que poco a poco va generando cambios o modificaciones en el conflicto de zona gris, lo cual puede crear un nuevo escenario de guerra híbrida o directa, según sea el caso, o, por el contrario, producir un hecho consumado que permita cumplir el objetivo estratégico.

Intereses sustanciales en juego

Esta característica de la guerra en zona gris es el motivo por el cual se genera el conflicto, ya que los intereses y beneficios que se quieren lograr son mayores a los riesgos que se corren si el enemigo o la amenaza los descubre. Es decir, en este

escenario se abandona la vía diplomática tradicional para adoptar estrategias que podrían cruzar líneas rojas, lo cual, de ser descubierto, podría acarrear sanciones o problemas diplomáticos graves para la nación, dependiendo de su peso geopolítico en el conflicto y de las alianzas que tenga con actores que puedan respaldarlo.

El efecto de la asimetría de intereses también se aprecia fuera de la zona gris, puntualmente en conflictos armados donde el débil vence al fuerte por razones similares (Mack, 1975). Asimismo, en la zona gris los intereses pueden ser antagónicos, por lo cual la respuesta por parte de las alianzas dependerá de si la amenaza los afecta de forma directa o si solo es un conflicto entre dos partes, por lo cual evitarán escalar el conflicto y procurarán ser neutrales para cuidar sus intereses nacionales.

Estrategias multidimensionales

Se puede decir que la guerra en zona gris tiene una gama de acciones o estrategias que se adaptan de acuerdo al tipo de guerra y los objetivos que se quieren cumplir. Específicamente, en este contexto las acciones pueden tener similitudes con la estrategia utilizada en la guerra híbrida, la cual ha incorporado un rango de diferentes modos de combatir, como "las capacidades convencionales, las formaciones y tácticas irregulares, los actos terroristas, incluyendo la violencia indiscriminada, la coerción y el desorden criminal" (Hoffman, 2007, p. 132). Todas estas acciones, que pueden ocurrir de forma "simultánea y adaptativa", se definen en un tipo de guerra multimodal utilizada y aprovechada por "Estados o grupos que seleccionan de todo el menú de tácticas y tecnologías y las mezclan de manera innovadora para encontrar su propia cultura estratégica, geografía y objetivos" (Hoffman, 2009, p. 5).

Se puede concluir que la guerra o el conflicto en la zona gris consiste en el empleo intencionado, multidimensional e integrado de diversos instrumentos de poder: políticos, económicos, sociales, informacionales, diplomáticos y también militares (Mazarr, 2015). En este escenario, la fuerza militar se usa de forma simbólica, con intención coercitiva, es decir, con el fin de señalar, intimidar y marcar territorio, o, en algunos casos, para respaldar a otros actores que están ejerciendo la fuerza. Sin embargo, se debe enfatizar en que la característica fundamental del conflicto en la zona gris es el empleo amplio e integrado de herramientas no armadas, pues si se emplea la fuerza militar para efectuar acciones ofensivas, el conflicto habrá escalado a una guerra abierta y directa, de modo que ya no se podría hablar del espectro de zona gris.

Dado que estas cuatro características son esenciales para determinar si existe un conflicto en zona gris, para la mayoría de la población civil es difícil determinar que existe un conflicto contra una amenaza que podría desestabilizar su estilo de

vida. Por lo tanto, buscar el apoyo de la opinión pública para legitimar los métodos o medios para atacar una amenaza o enemigo resulta ser una ardua tarea, de manera que es más práctico establecer alianzas regionales que comulguen con los mismos principios u objetivos para atacar dichas amenazas, pues, como dijo Waltz (2010), el sistema internacional se encuentra determinado por dos factores: el primero es la anarquía internacional, que es ausencia de una autoridad supranacional que garantice de manera efectiva la seguridad de los Estados, y el segundo es la distribución de poder relativo entre los Estados (Waltz, 2010).

Importancia operacional y estratégica de la Inteligencia militar en escenarios contemporáneos de guerra y conflictos de zona gris a nivel mundial y regional

Es importante tener clara la naturaleza del conflicto y de los actores que participan, ya que los procedimientos suelen cambiar dependiendo del impacto que se quiera obtener, bien sea a nivel táctico, operacional o estratégico, y de acuerdo con las directrices o intenciones del conductor de la guerra, quien sería el presidente o líder de la nación. En este escenario, las Operaciones de Inteligencia pueden obtener resultados estratégicos y de gran impacto nacional sin utilizar necesariamente un componente militar armado en su planeamiento o ejecución, de tal modo que se puedan evitar los riesgos de una confrontación armada, que sería mucho más grave en una guerra convencional entre dos o más países.

Por ende, la Inteligencia militar tiene un papel fundamental en el desarrollo de las guerras convencionales y no convencionales –en especial en la guerra en zona gris–, ya que las Operaciones de Inteligencia la proveen con las herramientas necesarias para recolectar la información, ya sea de carácter operacional o estratégico, que no solo ayuda a prevenir las intenciones o amenazas del adversario, sino que además brinda los insumos necesarios para planear las estrategias adecuadas a las capacidades enemigas y el ambiente operacional y estratégico en que está inmerso el conflicto.

Ahora bien, también se debe señalar que existe un elemento importante sobre la intencionalidad tramposa o fraudulenta en las acciones que efectúa el actor en la guerra de zona gris, ya que va en contravía del principio de buena fe que profesan los Estados en las relaciones internacionales (Baqués, 2017). Por ende, las

Operaciones de Inteligencia que se ejecutan en la zona gris deben tener un carácter de compartimentación y secreto operacional, lo cual restringe las posibilidades de que se transgredan los límites permitidos en esta zona y generar problemas que puedan escalar a un conflicto directo con el adversario.

En este punto ya se ha señalado a autores como Baqués (2017) o Jordán (2018), quienes se refieren explícitamente a la contravención del principio de la buena fe que debe regir en las relaciones internacionales como uno de los elementos relevantes del concepto. Así las cosas, las actuaciones en zona gris, si bien tratan de evitar a toda costa traspasar los límites establecidos, no pueden catalogarse como manifestaciones ordinarias, regulares y legítimas de las relaciones internacionales porque, precisamente, transgreden el principio de buena fe que las define.

Oportunidades en el uso de las Operaciones de Inteligencia y su aplicación en zonas grises en el desarrollo de las guerras contemporáneas

El conflicto o guerra en zona gris abre un abanico de posibilidades para efectuar Operaciones de Inteligencia acordes con la capacidad y el entrenamiento de las agencias de inteligencia. Asimismo, el factor económico desempeña un papel importante, pues no importa el tipo de operación que se quiera ejecutar, los recursos económicos determinan la duración y la continuidad de la actividad de inteligencia.

Específicamente, existen múltiples oportunidades o mecanismos que se pueden emplear en la zona gris, algunos de los cuales se presentan en los siguientes apartados.

Operaciones de influencia sobre la opinión pública del adversario y sobre la opinión pública internacional

Estas acciones se pueden enmarcar en las Operaciones de Inteligencia psicológicas o de información, en las cuales se crean o construyen narrativas que se puedan difundir a través de los medios de comunicación propios o del enemigo. De esta manera, se crean noticias o mensajes que fortalecen el punto de vista propio y se difama de la narrativa del adversario, para lo cual es importante emplear todos los tipos de redes sociales que puedan ser usados por el público o la audiencia objetivo.

En la actualidad existen varias empresas que generan tendencias en las redes sociales por medio de bodegas web o de información, en las cuales varias

personas utilizan computadores con múltiples perfiles falsos en las distintas plataformas, como Facebook, Twitter (ahora X), TikTok e Instagram, para posicionar de forma coordinada alguna tendencia o información de acuerdo con las necesidades del solicitante. Estas bodegas, también llamadas “granjas de *trolls* y de *clicks*”, comunes en algunos países, especialmente en Rusia, han afectado procesos electorales en Europa y los Estados Unidos. Con este propósito, también utilizan las *fake news* o noticias falsas, muy frecuentes en las redes sociales, lo que algunos ya denominan *deep fake*, e incluso podrían alterar videos muy creíbles para hacer que alguien diga y haga lo que necesitan (Marín, 2020). Estas herramientas son importantes, junto con la inteligencia artificial, para generar contenido informático creíble y de fácil entendimiento que genere la matriz de opinión favorable a nuestros intereses.

Asimismo, en el contexto regional deben existir medios de comunicación robustos y de buena reputación que puedan servir de caja de resonancia a las informaciones o noticias que se busca difundir, de manera que no se deben utilizar muchas *fake news* que puedan dañar su prestigio. En este sentido, la narrativa debe ser coherente con hechos reales que sean difíciles de refutar por parte de la contraparte. Finalmente, se debe tener en cuenta que en las áreas apartadas, donde no existe una influencia fuerte de los medios de comunicación escritos o digitales, la información llega por medio de mensajes de texto o cadenas de aplicaciones de mensajería instantánea.

En este contexto, aplicaciones como WhatsApp, Telegram, Facebook, Messenger, Signal, entre otros, son una herramienta para difundir cadenas de mensajes, videos o audios con información manipulada o *fake news* que ayudan a generar pánico o desinformación en las filas enemigas o en la población civil que les sean afectas. Por esta razón, constituyen un factor clave para golpear al enemigo por medio de operaciones de decepción que provoquen su desmovilización del frente de batalla o para asestar golpes fuertes contra su estructura armada por medio de unidades de Fuerzas Especiales.

Ciberataques contra entidades estatales y privadas

Estas acciones van encaminadas a interrumpir las actividades o funciones que cumplen las entidades privadas o públicas de un Estado u organización enemiga. Dado que es difícil identificar y responder a un ataque sin correr el riesgo de dañar o agravar las relaciones con otros Estados o con la contraparte en un conflicto (Silva, 2021), la respuesta apropiada de las autoridades correspondientes puede

ser deteriorar la credibilidad o la funcionalidad de las entidades ante su población civil para generar caos e incertidumbre.

Además, estas acciones sirven para robar información sensible que pueda brindar una ventaja estratégica importante sobre el adversario. Este es el caso del ciberespionaje económico, que puede ahorrar costos de inversión en investigación y desarrollo para un país si se apropia de los avances tecnológicos o la propiedad intelectual de productos de otras empresas o Estados para beneficio propio, como lo ha hecho China en los últimos años contra empresas occidentales.

Respaldo político a la oposición del gobierno adversario

Este método es utilizado por agencias de inteligencia estatales con la aprobación de los gobiernos para fracturar y perturbar el entorno político del adversario y, de este modo, debilitar su proceso de toma de decisiones. Uno de los casos domésticos más famosos fue el de Estados Unidos en 1901, cuando instigó una revuelta armada en los territorios colombianos del actual Panamá para favorecer su independencia y asegurar la construcción del Canal y el control de su área adyacente (Silva, 2021).

Este respaldo incluye aportar una ayuda financiera y los suministros necesarios para que la actividad política opositora sea exitosa, para lo cual es importante saber navegar en la zona gris de confrontación jugando con la ambigüedad de la situación. Por ende, es necesario no dejar huellas o pistas, como transacciones electrónicas o reuniones de la oposición política con agentes o enviados propios, de tal manera que se impida a las agencias de inteligencia o contrainteligencia enemigas obtener pruebas de este respaldo, lo cual reduce la posibilidad de escalar a un conflicto diplomático mayor.

Aquí vale la pena mencionar el caso de Viktor Medvedchuk, un político ucraniano del partido opositor prorruso Plataforma por la Vida, quien es el padrino de una de las hijas de Putin y fue apoyado activamente por la agencia de inteligencia rusa FSB para que creara las condiciones políticas para que Rusia invadiera a Ucrania en febrero del 2022. Mientras algunos analistas lo presentaban como el futuro enlace entre Rusia y una Ucrania derrotada y subyugada al Kremlin, y en Kiev lo llamaban “el príncipe de las tinieblas”, apodo que indicaba su tendencia a moverse en las sombras (Goncharenko, 2022), las agencias de inteligencia ucranianas le seguían los pasos por su evidente apoyo al Kremlin. Después de la fallida toma a Kiev por parte del ejército ruso, se escondió e intentó escapar hacia Rusia, pero fue capturado por los servicios de inteligencia ucranianos en abril del mismo año.

Es decir, solo el conductor estratégico político puede asumir el riesgo de apoyar una oposición política del adversario, pero debe hacerlo después de que haya analizado las consecuencias y, en lo posible, de forma tácita para que pueda avanzar en el cumplimiento de sus objetivos.

Acciones de inteligencia agresivas

Las actividades de inteligencia sobre el enemigo en un conflicto en zona gris se deben hacer de forma agresiva y constante para infiltrar sus servicios secretos de inteligencia, obtener información militar ultrasecreta de sus fuerzas militares o efectuar acciones violentas por medio de agentes reclutados para atacar las instituciones o personas que sean una amenaza para los intereses.

Como ejemplo se puede presentar el caso de las agencias de inteligencia rusas, las cuales efectuaron actividades agresivas de inteligencia en Colombia brindando apoyo al paro nacional en el año 2021. Así lo comprobó el *dossier* de la Central Intelligence Agency (CIA), que prueba el nexo de Rusia con los disturbios en Bogotá mediante su inyección de capital a grupos que estuvieron detrás de los desmanes y los destrozos en las protestas que acontecieron en todo el país, incluso en el año 2019 (*El Tiempo*, 2022). Esto indica que no importa la distancia geográfica que exista con el país objetivo para actuar en un conflicto en zona gris y mantener los intereses. En este caso, se trató de afectar la gobernabilidad del presidente de Colombia, fortalecer la oposición y generar un mejor panorama político al régimen venezolano, que en últimas es el principal aliado de Rusia en la región, junto con Nicaragua y Cuba.

Hechos consumados

Estos implican desafiar la disuasión del actor contrario, al que se busca provocar para forzarlo a que se sobreactúe, principalmente, de forma violenta, de manera que pierda legitimidad interna y externa para dejarlo en una posición forzada. Los referéndums o las declaraciones de independencia constituyen un buen ejemplo (Silva, 2021). Para que el hecho consumado funcione, la ganancia que se vaya a obtener debe ser limitada, de modo que la víctima prefiera dejar pasar estas acciones en lugar de iniciar una escalada que pueda iniciar una guerra armada.

Los hechos consumados son una estrategia común a la hora de ocupar territorios disputados entre dos o más Estados (Jordán, 2018). Por ejemplo, en la anexión de la península de Crimea, la Federación de Rusia utilizó una operación de engaño, ocupó con personal militar y agentes de inteligencia los centros de poder

de la región y desterró a las autoridades ucranianas. De esta manera, con un mínimo de fuerza obtuvo una ganancia territorial importante, lo que generó un hecho consumado que no pudo ser revertido por Ucrania ni la OTAN, ya que hubiera generado una escalada del conflicto con consecuencias graves para todos.

Guerras por delegación o (*proxy wars*)

También llamadas *guerras subsidiarias*, se producen cuando dos o más países utilizan a terceros como sustitutos y así evitar una confrontación de forma directa. Un caso reciente se presentó con el comienzo de la Guerra Fría, cuando la amenaza nuclear agitaba el espectro de una destrucción mutua asegurada, de manera que el recurso a los actores “delegados” comenzó a generalizarse entre las grandes potencias: la Unión Soviética, China y los Estados Unidos (Pontijas, 2020). Por ende, un Estado organizaba o apoyaba a otro Estado, ejército privado o bando en conflicto, brindándole armas, capacitación, entrenamiento militar, financiamiento y asesores, con el fin de que lucharan contra su enemigo sin emplear las fuerzas militares propias.

En la actualidad muchos países utilizan la guerra por delegación para mantener sus intereses, como Estados Unidos, Rusia, Reino Unido, Irán, Turquía, Arabia Saudí, China, Pakistán, entre otros. También lo utilizan actores no estatales, como grandes corporaciones y empresas, grupos terroristas, carteles de la droga, etc. (Pontijas, 2020), con la intención de desgastar las capacidades militares del enemigo en un conflicto armado y así erosionar o desmantelar sus capacidades militares por la confrontación bélica que está desarrollando contra su adversario.

En esta parte de la guerra en zona gris, un conflicto por delegación o *proxy wars* es aquel en el cual el enemigo puede tener claro las intenciones de su adversario y los objetivos que busca. Se trata de un método de guerra híbrida, casi de confrontación directa y que, dependiendo de las armas y los métodos de guerra que se utilicen, podría escalar a una guerra total. Esta es la situación que podría ocurrir en el conflicto entre Rusia y Ucrania, los cuales se encuentran inmersos en una guerra de carácter convencional directa, donde la OTAN, en cabeza de los Estados Unidos, ha enviado armas pesadas y apoyo económico importante para mejorar las capacidades de combate de las fuerzas militares ucranianas.

Esta estrategia ha servido para propinar golpes importantes contra el ejército ruso, de manera que el Kremlin tuvo que cambiar la estrategia y los objetivos que se había propuesto cuando inició sus acciones. Es decir, en lugar de ocupar Kiev y colocar un gobierno prorruso, como se había propuesto, su objetivo se transformó

en lograr el control del oriente del país, la región del Donbas, y arrebatarle la costa del mar negro a Ucrania.

Esta situación podría generar una peligrosa escalada bélica, pues Rusia podría interpretar el apoyo que la OTAN brinda a Ucrania como un acto beligerante, de manera que podría efectuar ataques contra Polonia o los países bálticos en una confrontación directa contra el poder de la organización, que es muy superior al poder militar ruso. Como evidencia este caso, que podría escalar a un conflicto nuclear, en una guerra por delegación se busca crear un conflicto directo con el adversario para debilitar sus capacidades militares y denegarle victorias en el campo de batalla, de tal manera que se logre erosionar su posición en una eventual negociación y preservar así los intereses y objetivos políticos que se plantearon.

Coerción económica

Son las medidas comerciales y financieras fuertes que se aplican contra Estados que se consideren hostiles o que estén interfiriendo en los intereses nacionales. Tienen el objetivo de golpear su capacidad de intercambio comercial internacional y el poder adquisitivo local de su población. Se debe resaltar que en este escenario tiene un papel importante el apoyo a las huelgas nacionales, sectoriales, individuales o coordinadas, entre otras acciones para ejercer una coerción política que refuerce la presión política (Silva, 2021). Estas medidas o sanciones económicas deben ser lo suficientemente fuertes como para que la presión que generan contra el gobierno adversario haga cambiar su posición política en un sentido favorable a los intereses del Estado que realiza las acciones.

Este es el caso de Venezuela, a la que Estados Unidos ha impuesto varias medidas de carácter económico y político para diezmar el poder del régimen, por ejemplo mediante sanciones económicas y el no reconocimiento de su presidencia. Aunque estas acciones han sido poco productivas, el gobierno de Maduro se ha visto forzado a hacer pequeñas concesiones políticas y a efectuar giros en materia económica para mantener el control del país. Específicamente, a través de un proceso de liberalización económica desordenada, ha intentado dar un respiro a la economía para beneficiar a sus élites y a grupos con acceso a divisas, con lo cual ha logrado minimizar las tensiones sociales. Esta transformación desordenada, en vez de debilitar a Maduro, le ha permitido consolidarse en el poder (Jiménez, 2022).

De igual manera, las sanciones contra países como Rusia, por su anexión ilegal de la península de Crimea en 2014, o a Irán en 2018, por su programa nuclear, no han sido efectivas porque estos países encontraron formas de compensar las

presiones externas sin renunciar a sus logros y objetivos. Además, sus medios de comunicación han usado estas sanciones como propaganda para denunciar una agresión a gran escala de Occidente que busca arrodillar al gobierno y la nación a sus caprichos. Estos hechos evidencian que, en un escenario de zona gris, la coerción económica se debe utilizar junto con otros métodos para lograr alguna ganancia estratégica sobre el enemigo.

Sliced salami tactics

Los orígenes del término, que en español se traduciría como “tácticas de corte salami”, se remontan por lo menos hasta finales de la década de 1940, cuando el líder comunista húngaro Mátyás Rákosi afirmó que había logrado derrotar a sus rivales internos incitándolos a abandonar segmentos cada vez más grandes de su propio partido, “cortándolos como rebanadas de salami” (Pusztai & Inántsyt-Pap, 2016). También llamado *obtención de ganancias graduales*, este mecanismo de guerra en zona gris se refiere al compendio o suma de varias acciones de bajo perfil que proporcionan ganancias graduales y que, a la vez, dificultan una reacción severa del adversario (Mazarr, 2015), pues, consideradas individualmente, no justifican su empleo de la fuerza. De esta manera es posible obtener una ventana de discusión o arreglo diplomático para buscar una solución sensata y evitar que el conflicto escale o se decante en una guerra.

Por lo tanto, las *sliced salami tactics* se generan cuando se han realizado varios hechos consumados para erosionar la posición del adversario y que han fortalecido nuestro poder de disuasión y posición en una posible negociación. De esta manera se habrá impedido que el enemigo reaccione, ya que su credibilidad estaría degradada en el momento en que decida actuar, lo cual agravaría su situación. Por ejemplo, Rusia ha efectuado tácticas salami de manera constante durante los últimos veinte años contra sus vecinos regionales, no solo al separar Abjasia y Osetia del Sur de Georgia, y a Crimea de Ucrania, sino también expandiendo sutilmente las vallas fronterizas en Georgia, realizando provocativos vuelos militares sobre Europa del Este y avanzando para controlar los recursos naturales del Ártico (Maass, 2022).

Finalmente, cabe señalar que las tácticas salami y los hechos consumados son exitosos si es posible controlar la ejecución de la escalada y se cuenta con las capacidades militares suficientes para imponerse en el nivel superior de conflicto.

Disuasión militar

Esta herramienta se puede considerar como la última medida disuasoria que se debe adoptar después de haber agotado las demás opciones disponibles, ya que su objetivo es efectuar acciones militares que logren un impacto psicológico en el enemigo. Para esto se demuestra que se cuenta con un poderío militar superior, de tal manera que genere temor al adversario en caso de querer escalar la confrontación o guerra en zona gris.

Como dice Jordán (2014), la disuasión es un proceso que consiste en influir en un actor mediante amenaza, tácita o explícita, con el fin de que no lleve a cabo una determinada acción. La disuasión se puede ejercer antes de que comience un conflicto, con el fin de evitarlo, pero también una vez que han estallado las hostilidades, con el propósito de limitar su alcance geográfico o el nivel de intensidad del enfrentamiento (Jordán, 2014). Por ello se debe evaluar de forma objetiva y profesional el coste/beneficio que podría traer esta acción al aplicarla.

Por otra parte, debe existir un conocimiento profundo de las capacidades militares del enemigo, sea estatal o no estatal, para poder diseñar estrategias de disuasión militar que eviten una escalada hacia una confrontación directa, la cual podría ocurrir por la falta de información sobre los protocolos de respuesta enemiga. Es decir, es fundamental tener claras la doctrina y las capacidades militares que tiene el adversario para contestar el ataque.

Finalmente, para concluir esta exposición, en la figura 1 se sintetizan las oportunidades o mecanismos que se pueden emplear en la zona gris.

Figura 1. Mecanismos que se pueden emplear en una zona gris.

ZONA GRIS	ESTRATEGIAS		OPERACIONES DE INTELIGENCIA
AMBIGÜEDAD	IMPACTAN	Operaciones de influencia sobre la opinión pública internacional y del adversario	ESPIONAJE
GRADUALISMO		Coerción económica	SABOTAJE
INTERESES SUSTANCIALES EN JUEGO		Acciones ofensivas de inteligencia	DECEPCIÓN
ESTRATEGIAS MULTIDIMENSIONALES		Guerras por delegación (proxy wars)	PSICOLÓGICAS
		Sliced salami tactics (obtención de ganancias graduales)	INFORMACIÓN
		Ciberataques contra entidades públicas y privadas	NEUTRALIZACIÓN

Fuente: Elaboración propia.

Zona gris en Colombia

Colombia se ha caracterizado en su historia republicana por combatir a grupos ilegales, estructuras de poder foráneas y comunidades locales que buscan tener el control político, social y económico por medios de la coerción militar o armada en las múltiples actividades ilícitas que suceden en el país. Al ser el primer productor de pasta base de coca del mundo, en el país existen múltiples organizaciones criminales que manejan los diferentes eslabones que intervienen en la producción de estupefacientes, como las disidencias de las FARC, el ELN, el Clan del Golfo, el EPL, grupos de delincuencia organizada regional, entre otros.

Asimismo, intervienen actores extranjeros que apoyan directa o indirectamente el tránsito de estupefacientes a cambio de dividendos económicos, como ocurre con el régimen venezolano, que es considerado por la comunidad internacional y por los organismos multilaterales como el principal puente de salida de la droga de Suramérica hacia otros destinos y continentes. Su situación política, económica y social, así como la corrupción, la inseguridad, la impunidad y el deterioro de los cuerpos de seguridad y de las instituciones del Estado han contribuido al incremento tanto del tráfico como del consumo de drogas en el país (Camero, 2017).

Sumado a esto, filtraciones de documentos reservados del 9 de agosto de 2019 del Servicio de Inteligencia Bolivariano (SEBÍN) y del Comando Estratégico Operacional de la Fuerza Armada Nacional Bolivariana (FANB) evidenciaron la presencia de las disidencias de las FARC y de miembros del ELN en territorio venezolano, los cuales contarían con el apoyo del presidente Nicolás Maduro (López, 2020). Este hecho provoca un grave problema de seguridad fronterizo con el vecino país, pues los grupos irregulares planean desde allí acciones armadas contra las Fuerzas Armadas y atentados contra la infraestructura crítica del Estado, con el objetivo de socavar la cohesión social de las comunidades y suplantar la autoridad del Estado. Además de esta grave situación, también se debe agregar el litigio marítimo entre Colombia y Nicaragua en la Corte Internacional de Justicia de La Haya por las fronteras marítimas del mar Caribe.

Este escenario suscita serios retos para la seguridad y la defensa del territorio colombiano, de manera que es necesario estudiar las diferentes estrategias multidimensionales que se podrían aplicar a estos grupos en una confrontación en la zona gris. Para cumplir este objetivo no son suficiente las acciones legítimas del Estado, como las operaciones militares o policiales, dirigidas a neutralizar a los miembros de las diferentes estructuras armadas que delinquen en el territorio

colombiano, sino que la estrategia también se debe direccionar a deslegitimar las acciones de estos grupos armados de cara a la población civil, que los ve como una autoridad legítima en sus territorios.

Por consiguiente, es posible evaluar la conveniencia de utilizar las operaciones de información o psicológicas para impactar a la población fronteriza y, por qué no, dirigirla contra los integrantes de los diferentes grupos armados para erosionar la confianza y la colaboración que puede existir entre estos. De esta manera, las acciones agresivas entre las estructuras podrían escalar al punto de que se instaure un ambiente propicio para la confrontación directa, lo cual afectaría sus componentes armados y la capacidad de recolección de finanzas que perciben de sus rentas ilegales. Todo esto sin poner en peligro la integridad de los miembros de las fuerzas de seguridad del Estado en una posible confrontación armada con dichas estructuras.

Ahora bien, las estructuras armadas están utilizando masivamente los medios de comunicación electrónicos, como los dispositivos móviles inteligentes, entre sus componentes armados y logísticos para coordinar el recaudo de finanzas y material logístico para su funcionamiento. Esta situación abre una ventana de oportunidad para aprovechar dicha debilidad y con ello obtener nuevas capacidades en equipos de guerra electrónica que brinden a las Fuerzas Armadas alcances novedosos, como la ubicación y hackeo de los equipos móviles, además de utilizar los ciberataques para robar datos y efectuar trabajos de judicialización o nuevas Operaciones de Inteligencia con la información recopilada.

Igualmente, dado que cada grupo armado que delinque en el país, dependiendo del área que controla, genera dinámicas propias de articulación y operatividad ilegal, resulta difícil proponer una estrategia general para atacarlas de forma homogénea. En este sentido, es necesario efectuar un estudio juicioso de las características físicas de terreno, población, infraestructura, vías de comunicación, control territorial, economías locales legales e ilegales, cobertura de los medios de información escritos o de televisión, sean regionales o nacionales, conectividad a servicios de internet y telefonía móvil, entre otros aspectos, con el propósito de analizar las posibles estrategias, no solo dirigidas a golpear la capacidad militar de las organizaciones criminales, sino también para atacarlas de forma integral, en especial quitándole el apoyo de la población civil y sus fuentes de financiamiento.

Por ello es fundamental tener claro el objetivo que se espera cumplir en una guerra en zona gris contra las estructuras criminales, ya que no existirá una victoria física para medir el éxito de la estrategia, sino que en este caso se buscaría

debilitar la capacidad estratégica que podrían tener los grupos armados ilegales y su control sobre áreas del territorio colombiano y la población civil que las habita.

Conclusiones

En un conflicto en zona gris es fundamental usar las Operaciones de Inteligencia como medio para cumplir los objetivos establecidos contra un Estado adversario u organización criminal, al tiempo que se busca preservar los intereses nacionales, como sea que los considere el tomador de decisiones estratégico. Con este propósito, se pueden emplear las operaciones de espionaje, sabotaje, decepción, psicológicas, neutralización o de información, con las cuales es posible impactar la zona gris y obtener ganancias estratégicas importantes sin necesidad de una confrontación armada directa.

Asimismo, existen varios retos en la zona gris, ya que su ambigüedad, intereses en juego y gradualismo hacen que se exploren diversas estrategias multidimensionales, las cuales se concretan con un estudio juicioso y completo del ambiente operacional de la amenaza. En el caso de Colombia, el país tiene problemas de seguridad fronteriza con Venezuela y un diferendo limítrofe con Nicaragua, así como un problema de seguridad interna, pues coexisten múltiples grupos armados que delinquen de diferentes formas. Por estas razones, se deben aplicar estrategias que ataquen su legitimidad como autoridad en las áreas donde operan, degradar el apoyo social que pueda existir en sus áreas de injerencia de manera diferencial y crear conflictos entre sus integrantes para afectar el mando y el control de estas estructuras. Además, es necesario atacar la zona gris con Venezuela y Nicaragua para fortalecer la posición estratégica de Colombia frente a los intereses que ellos buscan en nuestra nación.

Por último, se debe tener claro que la guerra en la zona gris es un conflicto entre las sombras, lo cual borra los límites que podrían existir entre paz y guerra entre naciones u organizaciones involucradas. Además, esta escala a un conflicto permanente o de larga duración que se libra de forma ambigua, por lo que en este espectro no se puede medir la victoria de forma física, sino las ganancias estratégicas que se logran sacar en procura de cumplir los objetivos para salvaguardar los intereses del Estado.

Referencias

- Andrade Rojas, W., Martínez Benavides, J. F., & Pineda Bello, J. C. (2011). *Las operaciones de información en las guerras de información* [Tesis de pregrado, Universidad Piloto de Colombia]. Repositorio UNIPILOTO. <https://tinyurl.com/3f7vpwer>
- Aznar, F. (2015, 25 de noviembre). *Las generaciones de guerras: Guerras de primera generación (I)* [Documento de Análisis, n.º 54]. Instituto Español de Estudios Estratégicos. <https://tinyurl.com/5yca9se5>
- Baqués, J. (2017). *Hacia una definición del concepto Gray Zone (GZ)* [Documento de Investigación, n.º 2]. Instituto Español de Estudios Estratégicos. <https://tinyurl.com/56aeyjde>
- Bolaños, L. F. L. (2018). El día que cambió la historia del arma nacional de Inteligencia. *Perspectivas en Inteligencia*, 10(19), 43-55. <https://doi.org/10.47961/2145194X.50>
- Camero, M. (2017). *El tráfico de drogas ilícitas en Venezuela*. Observatorio de Delito Organizado; Asociación Civil Paz Activa.
- Correa Martínez, S. L. (2017). *La estrategia antiterrorismo de los EE. UU. en Medio Oriente a partir de los atentados del 11S: Aproximaciones desde el mito político del excepcionalísimo norteamericano* [Tesis de pregrado, Pontificia Universidad Javeriana]. Repositorio PUJ. <https://tinyurl.com/4wf8f7dm>
- Cuneo, P. (2019). *Complejidad y multipolaridad en el Sahel: Nuevas dinámicas relacionales y de intervención en el marco de las relaciones internacionales* [Tesis de doctorado, Universidad Pontificia Comillas]. Repositorio Comillas. <https://tinyurl.com/ykknvmpy>
- Del Rey, V., & Canales Torres, C. (2012). *Blitzkrieg: La victoria alemana en la guerra relámpago* (vol. 1). EDAF.
- El Tiempo. (2022, 26 de marzo). El dossier de la CIA que prueba nexo entre rusos y disturbios en Bogotá. <https://tinyurl.com/hr7yjwcn>
- Gamboa, J. B. S. (2016). Ideas fundamentales sobre inteligencia. En *Inteligencia: Un enfoque integral* (pp. 13-40). Instituto Español de Estudios Estratégicos.
- Goncharenko, R. (2022, 14 de abril). Viktor Medvedchuk, el hombre de Putin en Ucrania. DW. <https://tinyurl.com/2kbh9afu>
- Hoffman, F. (2007). Conflict in the 21st Century: The rise of hybrid wars. Potomac Institute for Police Studies. <https://tinyurl.com/dyc5rmnv>
- Hoffman, F. (2009). Hybrid warfare and challenges. *Joint Force Quarterly*, 52(1), 34-39. <https://tinyurl.com/42ne9y2d>
- Jiménez, M. (2022). *El difícil camino hacia una democratización en Venezuela* [Documentos de Trabajo, n.º 61]. Fundación Carolina; Agenda 2030; Cooperación Española. <https://tinyurl.com/yc4f632w>
- Jordán, J. (2014, 18 de junio). Gestión de la incertidumbre en las relaciones internacionales: Dilema de seguridad, disuasión y diplomacia coercitiva. <https://tinyurl.com/4aw74fx9>

- Jordán, J. (2018). El conflicto internacional en la zona gris: Una propuesta teórica desde la perspectiva del realismo ofensivo. *Revista Española de Ciencia Política*, (48), 129-151. <https://tinyurl.com/3j5h2j39>
- Llop Meseguer, S., Martínez Enríquez, L., & Valeriano-Ferrer Gonzales, F. (2013). *Apuntes de inteligencia básica*. División de Publicaciones de la Escuela Superior e Guerra Naval. <https://tinyurl.com/4anuvwjy>
- López, C. (2020). Agencia, actores, escenarios: La tensa calma de la zona gris sudamericana. *Revista de Pensamiento Estratégico y Seguridad CISDE*, 5(2), 25-39. <https://tinyurl.com/vybftfy>
- Maass, R. W. (2022). Salami tactics: Faits accomplis and international expansion in the shadow of major war. *Texas National Security Review*, 5(1), 33-54. <https://tinyurl.com/29bc2jaa>
- Mack, A. (1975). Why big nations lose small wars: The politics of asymmetric conflict. *World Politics*, 27(2), 175-200. <https://doi.org/10.2307/2009880>
- Mazarr, M. J. (2015, 22 de diciembre). Struggle in the gray zone and world order. *War on the Rocks*. <https://tinyurl.com/5cakh86z>
- Méndez L. A., Gaitán Vanegas, S., & Fuquen, V. P. (2019). Los dominios de la guerra: Una aproximación al nuevo escenario de la Covid-19. *Estudios en Seguridad y Defensa*, 14(28), 237-257. <https://doi.org/10.25062/1900-8325.282>
- Muñoz Ciro, J. S. (2018). *Causas, proyecto político y medios del Estado Islámico* [Tesis de maestría, Universidad de Antioquia]. Repositorio UDEA. <https://tinyurl.com/5n8uxuvs>
- Pontijas, J. L. C. (2020). Tendencias en la guerra por delegación (proxy warfare). *Boletín IEEE*, (18), 85-96. <https://tinyurl.com/4ytzr357>
- Pusztai, G., & Inántszy-Pap, Á. (2016). An underground church-run school during the communist rule in Hungary (1948-1990). *Historia y Memoria de la Educación*, (4), 177-213. <https://doi.org/10.5944/hme.4.2016.15734>
- Quiñónez, R. I. G. (2012). *Curso básico de inteligencia*. S. p. i.
- Raggio, M. L. (2019). El conflicto en las sombras: Aspectos generales y elementos jurídicos de las operaciones en la zona gris. *Cuadernos de Estrategia*, (201), 17-56. <https://tinyurl.com/2yfnn3x>
- Sainz de la Peña, J. A. S. (1991). Estudio de "Inteligencia operacional". *Cuadernos de Estrategia*, (31), 15-37. <https://tinyurl.com/426wst5v>
- Schachtner, A. J. (2018). *Military intelligence in the gray zone: The strategic role of intelligence in unconventional warfare* [Tesis de maestría, US Army Command and General Staff College]. Repositorio DTIC. <https://tinyurl.com/9ccwwew8>
- Silva, J. S. (2021). La zona gris, un desafío para la conducción política y estratégica. *Cuaderno de Trabajo*, (6), 1-19. <https://tinyurl.com/593hxm3>
- Swenson, R. G., & Sancho, C. (Eds.). (2015). *Gestión de inteligencia en las Américas*. National Intelligence University. <https://tinyurl.com/y5uxkp2r>

Waltz, K. (2010). *Theory of international politics*. Waveland Press Inc.

Zavala, O. (2018). *Los cárteles no existen: Narcotráfico y cultura en México*. Malpaso Ediciones SL.

Capítulo 12

Capacidades ciber en los conflictos contemporáneos*

DOI: <https://doi.org/10.25062/9786287602809.12>

Juan David Zuleta

Andrés Acosta Muñoz

Escuela Superior de Guerra "General Rafael Reyes Prieto"

Resumen: Los eventos actuales demuestran que el conflicto cibernético ya es común en todo el mundo. Este capítulo aborda las estrategias y tácticas agresivas de la guerra cibernética en todas las etapas de la planificación de la seguridad y defensa nacionales. Se concluye que el liderazgo de seguridad y defensa nacional debe mejorar drásticamente su comprensión de la tecnología, la ley, la ética y los ataques cibernéticos, para que de esta manera se pueda tener en cuenta un contexto amplio de la guerra multidominio.

Palabras clave: defensa; estrategia, guerra ciber; inteligencia; seguridad.

* Este capítulo es resultado de investigación adscrito al proyecto "*Naturaleza de la guerra contemporánea. Retos y oportunidades de las Fuerzas Especiales y la Inteligencia*", adscrito al Departamento Ejército de la Escuela Superior de Guerra, inscrito en la línea de investigación "Naturaleza de la guerra, terrorismo, nuevas amenazas", que forma parte del grupo de investigación Centro de Gravedad, con código COL0104976. Los puntos de vista pertenecen a los autores y no reflejan necesariamente los de las instituciones participantes.

Juan David Zuleta

Teniente Coronel del Ejército Nacional de Colombia. Magíster en Seguridad y Defensa Nacionales, Escuela Superior de Guerra "General Rafael Reyes Prieto", Colombia. Especialista en Conducción y Administración de Unidades Militares, y Especialista en Administración de Recursos Militares para la Defensa Nacional, Escuela de Armas y Servicios del Ejército Nacional. Especialista en Administración Ecuestre, Escuela de Caballería del Ejército Nacional. Profesional en Ciencias Militares, Escuela Militar de Cadetes "General José María Córdova", Colombia. Contacto: juan.zuleta@buzonejercito.mil.co

Andrés Acosta Muñoz

Coronel del Ejército Nacional de Colombia. Magíster en Estrategia y Geopolítica, y especialista en Seguridad y Defensa Nacionales, Escuela Superior de Guerra "General Rafael Reyes Prieto", Colombia. Magíster en Seguridad y Defensa, Universidad de Nebrija, España. Especialista en Alta Gerencia, Universidad Militar Nueva Granada, Colombia.

<https://orcid.org/0000-0002-2813-5471> - Contacto: andres.acosta@esdeg.edu.co

Citación APA: Zuleta, J. D., & Acosta Muñoz, A. (2024). Capacidades ciber en los conflictos contemporáneos. En L. A. Montero Moncada & O. A. Garzón Gómez (Eds.), *Comandos: Retos de las Fuerzas Especiales e Inteligencia en la guerra contemporánea* (pp. 287-310). Sello Editorial ESDEG. <https://doi.org/10.25062/9786287602809.12>

COMANDOS: RETOS DE LAS FUERZAS ESPECIALES E INTELIGENCIA EN LA GUERRA CONTEMPORÁNEA

ISBN impreso: 978-628-7602-79-3

ISBN digital: 978-628-7602-80-9

DOI: <https://doi.org/10.25062/9786287602809>

Colección Seguridad y Defensa

Sello Editorial ESDEG

Escuela Superior de Guerra "General Rafael Reyes Prieto"

Bogotá D.C., Colombia

2024



Introducción

En este capítulo se abordan los conflictos contemporáneos, en los cuales se emplean las capacidades y los avances tecnológicos del dominio ciberespacial, tanto en la ofensiva como en la defensiva, para degradar las capacidades del adversario y generar un alto grado de desestabilización en el desarrollo de acciones militares antes, durante y después de un conflicto. Además, se analiza la importante participación de las unidades de Fuerzas Especiales (FF. EE.) e Inteligencia en el desarrollo de este tipo de acciones y operaciones cibernéticas, en la medida en que se están convirtiendo en la más importante tarea de los Estados para enfrentar a sus amenazas.

Al respecto conviene decir que el mundo está cambiando a pasos agigantados y que el desarrollo de las tecnologías de la información y las comunicaciones (TIC) avanza a un ritmo tan acelerado, que de alguna manera están superando las expectativas de las capacidades estratégicas, operacionales y tácticas de las Fuerzas Armadas en todo el mundo. La implementación de nuevas tecnologías desafía los parámetros y factores de las guerras convencionales, al tiempo que transforma las estrategias que los Estados adoptan para enfrentar a sus adversarios en los entornos nacionales, vecinales, regionales, continentales, hemisféricos y globales.

Siguiendo este criterio es posible identificar cuáles son las principales potencias en la temática, como ciertamente lo son Estados Unidos, China, Rusia, Israel e Irán, en la medida en que estos países son beligerantes en el ciberespacio y destinan recursos humanos, técnicos y económicos para desarrollar sus “ciberfuerzas”. En general, se puede afirmar que lo hacen con una doble intención: en primer lugar, garantizar la seguridad y la defensa de sus ciberespacios específicos y, en segundo lugar, ejercer poder e influencia entre sus ciudadanos, aliados y potenciales

adversarios (Colom et al., 2013). En últimas, todo esto tiene el propósito de prevenir y reaccionar ante la presencia de ataques cibernéticos que puedan poner en riesgo la continuidad y la disponibilidad de los servicios críticos del país.

No obstante, esto tan solo es la punta del iceberg. En la actualidad existen diferentes ramificaciones en los lineamientos estratégicos en los niveles ofensivo y defensivo, los cuales deben ser tratados para hacer frente a los diversos riesgos y amenazas que hay en el ciberespacio. En especial cuando se trata de los escenarios bélicos contemporáneos, en los cuales se requiere la intervención de unidades de FF. EE.

Además, este capítulo busca establecer la relación que tienen los nuevos requerimientos de las guerras contemporáneas en cuanto a la implementación del arte y el diseño operacional, con la identificación del centro de gravedad de las amenazas cibernéticas usando la inteligencia estratégica. Vale la pena aclarar que estos procesos iniciales de formulación y lógica “constituyen el sistema nervioso central de la doctrina del Ejército Nacional de Colombia y responde a las necesidades que tienen los comandantes y estados mayores de resolver situaciones en ambientes operacionales volátiles, inciertos, complejos y ambiguos” (Ejército Nacional de Colombia, 2019, p. 19).

Por otra parte, se evalúan las debilidades que tiene la concepción doctrinaria sobre el empleo de la Inteligencia y las capacidades cibernéticas en los conflictos contemporáneos mediante algunos estudios de caso. Esto significa que se analiza la relación entre las Operaciones de Inteligencia realizadas por medios cibernéticos, la tasa de éxito en el cumplimiento de los objetivos y los principales retos y desafíos que conlleva emplear herramientas cibernéticas en los escenarios contemporáneos.

Finalmente, se estudia el alcance de las estrategias y las Operaciones de Inteligencia militar en los conflictos y guerras contemporáneas desde varias perspectivas del dominio ciberespacial, con la finalidad de interpretar los propósitos, las características y los resultados de su desarrollo.

Metodología

La investigación se realizó con herramientas que permiten hacer un análisis comparativo de diversas teorías y eventos relacionados, lo cual implica un ejercicio

consistente de revisión bibliográfica sobre el tema y las capacidades cibernéticas empleadas en los conflictos contemporáneos. Además, se hace una investigación documental en la que se recopiló información sobre los lineamientos estratégicos a nivel ofensivo y defensivo.

De esta manera, se pudieron obtener registros de diversas fuentes bibliográficas, por ejemplo, en revistas, artículos científicos, libros, material archivado y otros trabajos académicos, lo cual permitió construir una visión general y particular de la naturaleza de la guerra contemporánea, los retos y las oportunidades de las FF. EE. y la Inteligencia. Si bien se trata de un estudio principalmente cualitativo que hace una conceptualización, evaluativa y observacional, también con apoyo en datos cuantitativos se explican los fenómenos observados mediante la recolección de datos digitales, los cuales son analizados con métodos que se basan en técnicas matemáticas, estadísticas o informáticas.

Posteriormente, se realiza un análisis comparativo y descriptivo de cada uno de los escenarios señalados, consistente en recolectar muestras con el propósito de observar el comportamiento de las diferentes variables expuestas como problema de investigación. Finalmente, se hace un análisis del discurso a varias series de documentos, especialmente políticas públicas y doctrina militar sobre las capacidades cibernéticas, con el fin de explicar el enfoque teórico que subyace en el concepto.

Los nuevos requerimientos de la guerra contemporánea

En la guerra contemporánea se encuentran varios escenarios y acontecimientos que contribuyen a formar una idea específica de cómo están evolucionando los conflictos armados. En otras palabras, existen razones para creer que los dominios de la guerra interactúan física y virtualmente. Así lo afirma Patrikarakos (2021), quien considera que hay dos guerras, una que se batalla en los dominios físicos (terrestre, marítimo, aéreo y espacial), y otra que se desarrolla en los entornos virtuales (ataques cibernéticos, sabotaje, desinformación y otro tipo de acciones). Estos aspectos hacen considerar que se presenta una nueva dinámica en los conflictos contemporáneos y, por lo tanto, nuevas necesidades para desestabilizar al adversario en tiempos de guerra y conflicto.

En este escenario, se ha despertado el interés de los gobiernos en todo el mundo por impactar, penetrar e influir las políticas sociales y económicas mediante el uso de las TIC. Como consecuencia, están identificando parcialmente las posibilidades, los retos y los desafíos que representa el amplio mundo del ciberespacio, al tiempo que expanden las estrategias y crean organizaciones de ciberdefensa y ciberseguridad, las cuales dedican sus esfuerzos a enfrentar las amenazas ciberespaciales. Esto quiere decir que las naciones están lidiando tan solo con la superficie de la "Cuarta Revolución Industrial" (Industria Conectada 4.0), la cual se caracteriza por una mezcla vanguardista de técnicas de producción con sistemas inteligentes, que se integran con las organizaciones y las personas, pero que a su vez cuentan con vulnerabilidades que son aprovechadas para generar alteración y daño en las infraestructuras críticas de una nación específica.

Al respecto conviene decir que las especialidades y necesidades de las fuerzas de seguridad y defensa han demandado varios cambios en las instituciones, los cuales han favorecido significativamente la protección de sus infraestructuras críticas. En otras palabras, las capacidades cibernéticas se han convertido en una tendencia que cada día toma más fuerza, al punto de fusionarse simbióticamente en las especialidades diferenciadoras de cada fuerza militar, generando innovaciones en sus organizaciones y plasmando una revolución positiva en el manejo de los riesgos y las amenazas a la seguridad nacional. Según Kenneth Geers (2009), "prácticamente todo lo que sucede en el mundo real se refleja en el ciberespacio. Para los planificadores de seguridad nacional, esto incluye propaganda, espionaje, reconocimiento, objetivos y, en una medida desconocida, la guerra misma" (p. 145).

Al respecto, conviene agregar que para Geers (2009) existen cinco tácticas comunes utilizadas en la guerra cibernética: el espionaje, la propaganda, la denegación de servicios (DoS), la modificación de datos y la manipulación de la infraestructura. En este contexto, se puede asegurar que el ciberespacio es, en definitiva, el "nuevo escenario de confrontación" entre Estados, naciones, democracias, dictaduras, organizaciones criminales, terroristas, entre otros.

Por esta razón hay una competencia entre potencias y países en vía de desarrollo para crear nuevas estructuras y organizaciones facilitadoras que permitan, por un lado, proteger las capacidades informáticas propias y, por otro, ser capaces de realizar operaciones cibernéticas con diferentes objetivos, principalmente orientados a afectar las capacidades de las amenazas. Por lo tanto, en este punto se puede decir que surge la ciberguerra.

Con base en este panorama, a continuación se desarrolla la Metodología de Diseño del Ejército (MDE) para definir la estructuración de un ambiente operacional (AO) desde una perspectiva sistémica durante el proceso de operaciones, relacionado con las capacidades cibernéticas en los conflictos contemporáneos. Con este propósito se empleará una serie de diagramas de análisis de red para visualizar y describir el ambiente, lo cual permite mostrar de manera sencilla y didáctica las conexiones que existen en las diferentes redes para entender el AO en torno a los riesgos y las amenazas en el dominio ciberespacial.

Vale la pena aclarar que el AO es definido por el Ejército Nacional de Colombia (2017b) como la “composición de condiciones, circunstancias e influencias que afectan el empleo de las capacidades y que pesan en las decisiones del comandante” (p. 1-2). Desde esta perspectiva, en los siguientes apartados se enmarca el problema operacional, es decir, se presenta una situación general de los aspectos representativos en los conflictos contemporáneos, los cuales estarán relacionados con los lineamientos estratégicos a nivel ofensivo y defensivo en el dominio ciberespacial, así como con la estructura en el enfoque operacional.

Guía de Planeamiento Estratégico 2018-2022

En el *Plan Estratégico del Sector Defensa y Seguridad - Guía de Planeamiento Estratégico 2018-2022 (PES)*, el Ministerio de Defensa Nacional (MDN) emitió instrucciones a las Fuerzas Militares para direccionar “la misión constitucional de la fuerza pública y la consecución de los objetivos estratégicos nacionales” (MDN, 2018, p. 3). Además, establece la hoja de ruta de la planeación integrada del sector defensa y seguridad durante el cuatrienio, partiendo del análisis de las amenazas y los retos a la defensa y la seguridad nacionales. Específicamente, estas fueron las premisas que el MDN (2018) dio a las Fuerzas Militares:

1. Los riesgos y las amenazas al Estado en el ciberespacio representan una nueva preocupación, dado que pueden provenir de diferentes actores, de cualquier parte del mundo, y buscan cumplir objetivos asociados a diversos fenómenos, como la criminalidad, el espionaje, el sabotaje, el terrorismo, entre otros (MDN, 2018, p. 8).
2. Frente a los retos y las amenazas presentados en el ámbito externo, el *Plan Estratégico del sector Defensa y Seguridad - Guía de Planeamiento Estratégico 2018-2022 (PES)* propone la defensa de los intereses nacionales a través de una estrategia robusta que, adicionalmente, fortalezca

las capacidades en seguridad digital, ciberdefensa, inteligencia y contra inteligencia (MDN, 2018, p. 9).

Situación general

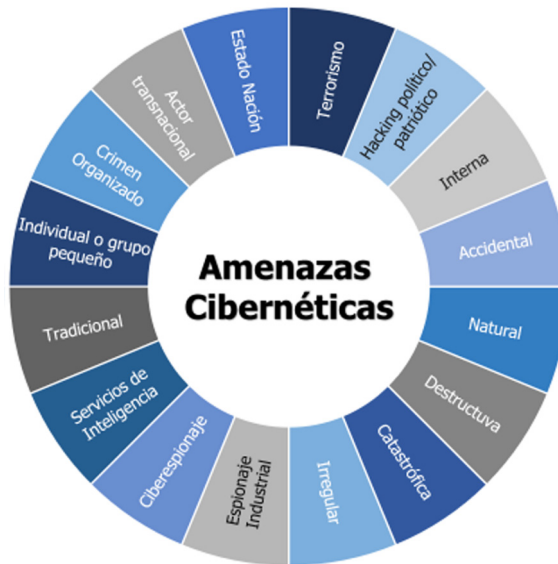
En 1962, el Departamento de Defensa de los Estados Unidos, a través de la Agencia de Investigación de Proyectos Avanzados (ARPA, por la sigla en inglés de *Advanced Research Projects Agency Network*), solicitó el desarrollo de una tecnología que permitiera la comunicación interconectada entre diferentes instituciones gubernamentales. Posteriormente, en 1969, se logró exitosamente la prueba de mensaje, con la cual se creó la primera red de comunicación entre la Universidad de Stanford y la Universidad de California en los Ángeles (UCLA).

Después, en el año de 1988, hizo su aparición el primer código o software malicioso del mundo, el cual fue denominado con el nombre de *Worm Morris* ('Gusano Morris'). Al ser el primero en su especie, generó estragos en las redes computacionales y en los ordenadores de la época. Contaba con la capacidad de autorreplicarse rápidamente, de manera que logró una afectación directa al internet. El impacto que generó en los sistemas informáticos permitió evidenciar las vulnerabilidades de la internet. Todo esto exigió a los desarrolladores definir protocolos de seguridad que protegieran las redes informáticas de futuros ataques devastadores. Por lo tanto, los hechos ocurridos en ese año abrieron un campo de oportunidades para crear una variedad inimaginable de malwares, lo cual cambió significativamente las posibilidades de interacción de los sistemas informáticos. De esta manera surgieron los ciberataques y el ciberespionaje.

En 1990, el Consejo Europeo para la Investigación Nuclear (CERN, por la sigla en francés de *Centre Européen de Recherche Nucléaire*), junto con varios físicos ubicados en Ginebra y Suiza, desarrollaron el lenguaje HTML (lenguaje de marcado hipertextual) y el mismo año también se creó el primer cliente web o la World Wide Web (WWW).

Ahora bien, en la década actual (2020-2030) existen diversos agentes de la amenaza del dominio ciberespacial (figura 1), los cuales tienen diferentes tipos o múltiples finalidades, como motivos económicos, políticos, intelectuales, inteligencia, espionaje industrial, entre otros. Aún así, el riesgo más grande proviene de los Estados y las organizaciones de inteligencia, que, mediante la manipulación de estructuras o grupos de diferente índole, ejecutan sus actividades en busca de cumplir objetivos específicos.

Figura 1. Amenazas cibernéticas.



Fuente: Elaboración propia.

Las amenazas más recurrentes en el ciberespacio se pueden catalogar de acuerdo con las siguientes denominaciones: amenaza Estado-nación; amenaza actor transnacional; amenaza crimen organizado; amenaza individual o de grupos pequeños; amenaza tradicional; servicios de inteligencia; ciberspionaje; espionaje industrial; amenaza irregular; amenaza catastrófica; amenaza destructiva; amenaza natural; amenaza accidental; amenaza interna; *hacking* político/patriótico y terrorismo.

Estructura del ambiente operacional

La nueva tipología de batalla está enmarcada en la posguerra fría, en la cual se planteó la empleabilidad de los computadores y las comunicaciones en la red para enfrentar las amenazas mediante el desarrollo y la ejecución de información con propósitos psicológicos y de desarticulación logística. Asimismo, se caracteriza por emplear tecnologías de la información en diferentes organizaciones de nivel estratégico, operacional y táctico, los cuales tienen una infinidad de componentes y recursos de las fuerzas armadas a nivel global.

En los Estados Unidos, que prácticamente son considerados la cuna del internet, varios pensadores, militares, políticos, etc., están invirtiendo tiempo y recursos para analizar la fenomenología de los riesgos y las amenazas cibernéticas, así

como las alternativas que les sean necesarias para logran mantener el liderazgo frente al entorno global del dominio ciberespacial.

Por su parte, la Organización del Tratado del Atlántico Norte (OTAN) define que la infraestructura crítica de un país está compuesta por instituciones públicas y privadas de los sectores de la agricultura, los alimentos, el agua, la salud pública, los servicios de emergencia, el gobierno, la industria de defensa, la información y las telecomunicaciones, la energía, el transporte, la banca y las finanzas, los productos químicos y materiales peligrosos y la administración postal (Geers, 2009).

Además, se considera que el ciberespacio es el sistema nervioso, el sistema de control de un país. El ciberespacio está formado por cientos de miles de ordenadores interconectados, servidores, enrutadores, concentradores y cables de fibra óptica que permiten fusionar la infraestructura crítica. Por esta razón, el funcionamiento saludable del ciberespacio es esencial para la economía y la seguridad nacionales.

Identificación del problema y el desarrollo de opciones

Las razones estratégicas por las cuales la guerra cibernética está en aumento se relacionan con varios factores preponderantes. En primer lugar, la internet es vulnerable a los ataques cibernéticos. Indiscutiblemente no existe seguridad que garantice al cien por ciento su invulnerabilidad. Por lo tanto, en la actualidad se puede afirmar que no existe un sistema totalmente seguro en el mundo, el cual sea capaz de evitar los diferentes tipos de ataque cibernéticos. Además, el diseño imperfecto de internet permite a los hackers leer, eliminar y/o modificar subrepticamente la información almacenada o enviada entre computadores. Por lo tanto, los ataques, armados con código malicioso en constante evolución, probablemente tengan más rutas de acceso a su red y los secretos que contiene de las que los administradores del sistema pueden proteger.

En segundo lugar, se encuentra el alto retorno de la inversión. Los objetivos de los practicantes de la guerra cibernética hablan por sí mismos: el robo de datos de investigación y desarrollo, el espionaje de comunicaciones sensibles y la entrega de propaganda. Lo distintivo de la piratería informática radica en el hecho de que se puede intentar por una fracción del costo y el riesgo de cualquier otra estrategia de recopilación o manipulación de información.

En tercer lugar, la insuficiencia de la ciberdefensa. La defensa cibernética sigue siendo una disciplina inmadura, aunque en constante evolución. Las habilidades tradicionales de aplicación de la ley son inadecuadas, y es difícil retener al personal

con habilidades altamente comercializables. Las investigaciones informáticas desafiantes se complican aún más por la naturaleza internacional de internet. Finalmente, no existen operaciones ofensivas en el ciberespacio patrocinadas por los Estados ni cooperación entre las fuerzas del orden.

En cuarto lugar, se encuentra la negación plausible. La arquitectura laberíntica de internet ofrece a los ciberatacantes un alto grado de anonimato. Los hackers inteligentes pueden enrutar ataques a través de países con los que el gobierno de la víctima tiene malas relaciones diplomáticas y no coopera con las fuerzas del orden. Incluso las investigaciones exitosas a menudo conducen solo a otra computadora pirateada. Los gobiernos de hoy se enfrentan a la perspectiva de perder un conflicto cibernético sin conocer nunca la identidad de su adversario.

Por último, y en quinto lugar, se encuentra la participación de agentes no estatales. Los Estados-nación se esfuerzan por mantener tanto control como puedan sobre los conflictos internacionales, pero la globalización y la internet han fortalecido considerablemente la capacidad de cualquier persona para seguir los acontecimientos actuales, así como el poder para darles forma. Las subculturas transnacionales ahora se fusionan espontáneamente en línea e influyen en innumerables agendas políticas, sin informar a ninguna cadena de mando. En este sentido, un desafío para el liderazgo de la seguridad nacional es que esta actividad podría poner a la delicada diplomacia fuera de control.

Estos fenómenos parecen confirmar que todos los conflictos políticos y militares tienen una dimensión cibernética, cuyo tamaño e impacto son difíciles de predecir, pues los atacantes tienen a su disposición una amplia variedad de estrategias y tácticas efectivas de guerra cibernética.

Por lo tanto, internet es vulnerable a los ataques de naturaleza cibernética. Además, su poder amplificador significa que las futuras victorias en el ciberespacio podrían traducirse en victorias sobre el terreno. Tanto los actores estatales como los no estatales disfrutan de un alto retorno de la inversión en tácticas cibernéticas, que van desde la colocación de propaganda cuidadosamente elaborada hasta la manipulación de la infraestructura crítica del adversario.

Las debilidades en la concepción doctrinaria

La concepción doctrinaria de las fuerzas militares a nivel mundial referente a este tipo de temas se encuentra en etapas muy tempranas, así que existe un largo camino por recorrer para comprender y establecer normativas que permitan

implementar estrategias, métodos, procedimientos y tácticas para enfrentar los riesgos y las amenazas en el ciberespacio. Como consecuencia, es necesario establecer algunos factores importantes para desarrollar una aproximación doctrinaria que permita enfrentar estos desafíos. A continuación, se identifica su empleo en la Inteligencia, las capacidades cibernéticas en los conflictos contemporáneos y estudios de caso que permiten caracterizar algunos aspectos que se deben tener en cuenta en este tipo de iniciativas.

Empleo de la Inteligencia

Sin lugar a duda, las capacidades que brindan las herramientas de la guerra cibernética para los estamentos de seguridad y defensa en el campo de la inteligencia son excepcionales. Por lo tanto, es posible asegurar que estas capacidades siguen siendo una gran posibilidad para lograr una ventaja estratégica con respecto a los adversarios. La infiltración, penetración y captación de información son sus principales ventajas, pues garantizan las puertas de acceso furtivas necesarias para alcanzar con éxito las Operaciones de Inteligencia.

Capacidades ciber en conflictos contemporáneos

Según Patrikarakos (2021), “los términos como guerra híbrida, desinformación y granja de *trolls*, se han convertido en palabras de moda en nuestra era de la pos-verdad” (p. 14). Sumado a esto, actualmente la probabilidad de controlar la internet, el tráfico, los móviles, los sistemas de seguridad, etc., no es un cuento de ciencia ficción, sino, más bien, parte del concepto general de la ciberguerra. Por esta razón, “los estrategas deben ser conscientes de que parte de todo conflicto político y militar tendrá lugar en internet” (Geers, 2009, p. 58).

Los ataques cibernéticos han mejorado e incrementado su capacidad y complejidad; año tras año un nuevo virus, troyano o software malicioso aparece en escena. Habilidades características para interrumpir procesos, abrir puertas traseras, modificar códigos, facilitar el robo de información, recolectar información de las relaciones comerciales de diferentes organizaciones y degradar sistemas son la señal de que las características del ciberespacio hasta ahora están en pleno descubrimiento.

Por lo tanto, se debe reconocer que no existe ninguna aplicación de software que no tenga vulnerabilidades. En otras palabras, los sistemas industriales, comerciales, militares, gubernamentales, policiales, etc., requerirán de una mayor atención, preferiblemente, por el impacto que representa cada una de las categorías y

la manera inmediata en que pueden afectar las infraestructuras críticas. Debido a estas características, se pueden convertir en objetivos de muchas organizaciones, en especial de grupo de hackactivistas, cibercriminales, ciberterroristas, Estados, entre otros. Es importante dejar claro que los efectos de estos ataques serían devastadores para las infraestructuras críticas de cualquier nación.

Estudios de casos

A continuación, se presentan varios estudios de casos relacionados con las capacidades cibernéticas en los conflictos contemporáneos, los cuales permiten identificar, evaluar y analizar, en el entorno general del ciberespacio, los riesgos y las amenazas a las cuales se enfrentan las instituciones de seguridad y defensa nacionales.

Chechenia (1994)

En la era de internet, las noticias sin editar de un frente de guerra pueden llegar en tiempo real. Los usuarios de internet de todo el mundo desempeñan un papel importante en los conflictos internacionales al publicar información, ya sea en formato de texto o imagen, en un sitio web.

Según Thomas Timothy (2003), desde los primeros días de la World Wide Web, las fuerzas prochechenas y prorrusas han librado una guerra virtual en internet, la cual se desarrolla simultáneamente en los campos de batalla reales. El movimiento separatista checheno, en particular, es considerado un pionero en el uso de la web como una herramienta para entregar poderosos mensajes de relaciones públicas. La hábil colocación de propaganda y otros tipos de información, como el número de una cuenta de banco para recaudar fondos de guerra en Sacramento, California, ayudó a unir a la diáspora chechena.

Además, la información más efectiva, sin embargo, no era prochechena, sino antirrusa. Las imágenes digitales de cadáveres ensangrentados sirvieron para poner a la opinión pública en contra de los supuestos excesos militares rusos. En 1999, justo cuando los funcionarios del Kremlin negaban un incidente en el que un autobús checheno fue atacado y muchos pasajeros murieron, las imágenes del incidente aparecieron en la web. A medida que avanzaba la tecnología, los internautas veían videos en *streaming* referentes a la actividad militar chechena de manera favorable, como fueron las emboscadas a convoyes militares rusos (Goble, 1999).

Cabe aclarar que, según Goble (1999), el gobierno ruso admitió la necesidad de mejorar sus tácticas en el ciberespacio. En 1999, Vladimir Putin, entonces primer ministro de Rusia, declaró: “Entregamos este terreno hace algún tiempo... pero ahora estamos entrando en el juego de nuevo” (Goble, 1999, s. p.). Moscú buscó la ayuda de Occidente para cerrar el importante sitio web prochecheno kavkaz.org, y anunció “la introducción de la censura militar centralizada con respecto a la guerra en el Cáucaso norte” (s. p.).

Por lo tanto, según Bullough (2002), durante la segunda guerra chechena (1999-2000), los funcionarios rusos fueron acusados de escalar el conflicto cibernético, pirateando sitios web chechenos. El momento y la sofisticación de al menos algunos de los ataques sugirieron la participación del Estado-nación, por ejemplo kavkaz.org, que estaba alojado en los Estados Unidos. Según los informes, fue desconectado simultáneamente al asalto por parte de las fuerzas especiales rusas, quienes adelantaban una operación de rescate en el interior de un teatro de Moscú sitiado por terroristas chechenos.

Kosovo (1999)

En los conflictos globalizados de la era de internet, cualquier persona con una computadora y una conexión a internet es un combatiente potencial. El primer gran compromiso militar de la OTAN siguió al crecimiento explosivo de la web durante la década de 1990. Así como Vietnam fue la primera guerra televisada del mundo, Kosovo fue su primera guerra de internet a gran escala.

Según Geers (2020), a medida que los aviones de la OTAN comenzaron a bombardear Serbia, numerosos grupos de hackers proserbios (o antioccidentales), como la Mano Negra, comenzaron a atacar la infraestructura de internet de la OTAN. Se desconoce si alguno de los hackers trabajó directamente para el ejército yugoslavo; en cualquier caso, su objetivo declarado era interrumpir las operaciones militares de la OTAN.

La Mano Negra, que tomó prestado su nombre de la sociedad secreta paneslava que ayudó a iniciar la Primera Guerra Mundial, afirmó que podían enumerar las computadoras “más importantes” de la OTAN, y que, a través de la piratería, intentaría “eliminar los datos” que contenían. El grupo adjudicó su éxito en al menos algunos puntos vulnerables, por lo menos en computadores de la Marina estadounidense, y declaró que posteriormente fue sacado de línea.

Los computadores de la OTAN, los Estados Unidos y el Reino Unido fueron atacados durante la guerra a través de la denegación de servicio y el correo electrónico

infectado por virus (se detectaron veinticinco cepas diferentes de virus) (Geers, 2020). En los Estados Unidos, el sitio web de la Casa Blanca fue desfigurado y se inició una investigación por parte del Servicio Secreto. En este escenario, mientras que los Estados Unidos afirmaban no haber sufrido “ningún impacto” en el esfuerzo de guerra general, el Reino Unido admitió haber perdido al menos parte de la información de la base de datos.

En el cuartel general de la OTAN en Bélgica, los ataques se convirtieron en una victoria propagandística para los hackers. El sitio web de asuntos públicos de la OTAN para la guerra en Kosovo, donde el organismo trató de retratar su lado del conflicto a través de sesiones informativas y actualizaciones de noticias, fue virtualmente inoperante durante varios días. El portavoz de la OTAN, Jamie Shea, culpó de la “saturación de la línea” a los “hackers en Belgrado”. Una avalancha simultánea de correo electrónico ahogó con éxito el servidor de correo electrónico de la OTAN. A medida que la organización se esforzaba por actualizar casi todos sus servidores informáticos, los ataques a la red, que inicialmente comenzaron en Belgrado, se expandieron por todo el mundo.

Oriente Medio (2000)

Durante la Guerra Fría, el Oriente Medio sirvió a menudo como campo de pruebas para armas y tácticas militares. En la era de internet se ha hecho lo mismo con la guerra cibernética.

En octubre de 2000, tras el secuestro de tres soldados israelíes, se plantaron banderas azules y blancas y un archivo de sonido que reproducía el himno nacional israelí en un sitio web pirateado de Hezbolá. Los ataques proisraelíes posteriores se dirigieron a los sitios web oficiales de organizaciones militares y políticas percibidas como hostiles a Israel, incluyendo la Autoridad Nacional Palestina, Hamas e Irán (Preatoni, 2014).

Las represalias de los hackers propalestinos fueron rápidas y mucho más diversas en su alcance. La política, el ejército, las telecomunicaciones, los medios de comunicación y las universidades israelíes se vieron afectados. Los atacantes también ejecutaron acciones en contra de sitios de valor económico puro, incluido el Banco de Israel, sitios de comercio electrónico y la Bolsa de Valores de Tel Aviv. En ese momento, Israel estaba más conectado a internet que todos sus vecinos combinados, por lo que no había escasez de objetivos. El dominio “.il” proporcionó una lista bien definida que los hackers propalestinos trabajaron metódicamente.

Como se observa, las guerras a menudo muestran nuevas herramientas y tácticas. Específicamente, durante este conflicto el programa DoS "Defender" fue utilizado con gran efecto por ambas partes, demostrando en parte que el software se puede desestabilizar más rápidamente que un tanque o un rifle. La innovación de defensa fue revisar continuamente la fecha y hora de sus solicitudes web simuladas, lo cual sirvió para derrotar los mecanismos de seguridad de almacenamiento en caché web de la época (Geers, 2004).

Por lo tanto, la guerra cibernética de Oriente Medio demostró que el portal de la era internet y los conflictos políticos pueden internacionalizarse rápidamente. Por ejemplo, según BBC News (2000), Pakistán "Hackers Club" penetró en el lobby proisraelí con sede en Estados Unidos (AIPAC, por la sigla en inglés de American Israel Public Affairs Committee), y publicó correos electrónicos confidenciales, números de tarjetas de crédito e información de contacto de algunos de sus miembros. Asimismo, Barnaby Page (2000) afirmó que "la firma de telecomunicaciones AT&T fue blanco de ataques por proporcionar apoyo técnico al gobierno israelí durante la crisis" (s. p.).

Además, Rebecca Anna Stoil y James Goldstein (2006) aseguraron que la guerra cibernética de Oriente Medio ha continuado generalmente en el ciberespacio y no se ha detenido hasta la fecha. En 2006, a medida que aumentaban las tensiones entre Israel y Gaza, los piratas informáticos propalestinos cerraron alrededor de setecientos dominios de internet israelíes, incluidos los de Bank Hapoalim, Bank Otsar Ha-Hayal, BMW Israel, Subaru Israel y McDonalds Israel.

Estados Unidos y China (2001)

El 26 de abril de 2001, el Centro Nacional de Protección de Infraestructura (NIPC, por su sigla en inglés) de la Oficina Federal de Investigaciones (FBI) publicó el aviso 01-009:

Citando eventos recientes entre los Estados Unidos y la República Popular China (PRC), los hackers han intensificado sus ataques dañando páginas web. Esta actividad busca dañar a la red, y a los administradores de servicios sensibles. Allí es donde hay una mayor actividad de piratas informáticos dirigidos a Estados Unidos y sus sistemas más sensibles [...]. Los hackers chinos discutieron públicamente el aumento de su actividad durante este período, que coincide con fechas históricas importantes en la República Popular China. (Information Warfare Site [IWS], 2001, p. 86; traducción propia)

Las tensiones habían aumentado considerablemente entre los dos países después de que Estados Unidos bombardeara la embajada china en Belgrado en 1999, y después de la colisión en el aire de un avión de la Armada estadounidense y un avión de combate chino sobre el Mar del Sur de China en 2001, seguido de la detención prolongada de la tripulación estadounidense en la República Popular China.

Según Jeremy Wagstaff (2001), reportero del *The Wall Street Journal*, los hackers de ambos lados del Pacífico, como China Eagle Alliance y PoizonB0x, comenzaron la desfiguración de sitios web a gran escala y construyeron portales de hackers con títulos como "USA Kill" y "China Killer". Cuando terminaron las escaramuzas cibernéticas, ambas partes reclamaron difamaciones y DoS en infinidad de oportunidades.

En este contexto, el FBI investigó un hackeo de 17 días a una red de prueba de la red de energía eléctrica de California que comenzó el 25 de abril (Weisman, 2001). El caso fue ampliamente desestimado como exageración de los medios en ese momento, pero la CIA informó a los líderes de la industria en 2007 que no solo es posible una amenaza tangible de piratas informáticos para tal infraestructura crítica, sino que, de hecho, ya había sucedido (Nakashima & Mufson, 2008).

Estonia (2007)

El 26 de abril de 2007, el gobierno estonio trasladó un monumento soviético de la Segunda Guerra Mundial fuera del centro de su capital, Tallin, en un movimiento que inflamó la opinión pública tanto en Rusia como entre la población minoritaria rusa de Estonia.

A partir del 27 de abril, el gobierno de Estonia, las fuerzas del orden, la banca, los medios y la infraestructura de internet sufrieron tres semanas de ataques cibernéticos, cuyo impacto aún genera un gran interés por parte de gobiernos de todo el mundo.

Debido a que los estonios realizan más del 98 % de sus operaciones bancarias en línea, se entiende el impacto de múltiples ataques distribuidos de DoS, que cortaron todas las comunicaciones a los dos bancos más grandes del país durante hasta dos horas y lograron que los servicios internacionales prestados parcialmente no quedaran disponibles durante días.

Menos discutidos, pero probablemente de mayor consecuencia, tanto para los planificadores de seguridad nacional como para el personal de defensa de la red informática, fueron los ataques a la infraestructura de internet (enrutador) en los

ISP del gobierno estoniano, que se dice interrumpieron las comunicaciones del gobierno durante al menos un período de tiempo “corto”.

En el frente de la propaganda, un hacker desfiguró el sitio web del partido político del primer ministro estonio el 27 de abril, cambiando el texto de la página a una supuesta disculpa fabricada por el gobierno por haber movido la estatua, junto con la promesa de volver a su original ubicación.

Hubo un gran interés diplomático en este ataque cibernético debido en parte a la posible reinterpretación del artículo 5.º de la OTAN, según el cual “un ataque armado contra un [miembro de la Alianza] [...] se considerará un ataque contra todos ellos” (OTAN, 1949, art. 5.º). Cabe señalar que el artículo 5.º solo se ha invocado una vez, luego de los ataques terroristas del 11 de septiembre de 2001. Potencialmente, algún día podría interpretarse que abarca también los ataques cibernéticos.

Irán (2010)

Uno de los casos más representativos en la era de la guerra cibernética es el de Irán. Sin lugar a duda el desarrollo del gusano Stuxnet se convirtió en la herramienta capaz de afectar gravemente la infraestructura crítica de esta nación. Específicamente, este ataque tenía el objetivo de interrumpir las actividades nucleares que se llevaban a cabo en el reactor de Bushehr. Aquí vale la pena decir que el objetivo se cumplió satisfactoriamente, pues se logró generar un significativo retraso en el programa nuclear iraní.

Las características especiales de este caso dan cuenta de que toda su ejecución cumple las condiciones perfectas de una ciber guerra. Por esta razón, se podría inferir que la creación de esta ciber arma es en definitiva una herramienta que logró afectar los intereses nacionales de Irán. Además, establecer una operación de infiltración y de engaño para activarla y afectar las redes informáticas de un país y dejarlo vulnerables frente a ataques de cualquier naturaleza (Porteus, 2010), solo puede ser catalogado como ingenioso e innovador.

Ucrania (2014)

Ucrania fue el laboratorio de nuevos tipos de operaciones de información (Patrikarakos, 2021). El 21 de noviembre de 2013, Mustafá Nayyem, un periodista ucraniano de ascendencia afgana, escribió una publicación en Facebook instando a la gente a reunirse en Maidan Nezalezhnosti (Plaza de la Independencia) de Kiev. Quería protestar contra la decisión del presidente Viktor Yanukovich de dar marcha

atrás en su compromiso de firmar un acuerdo de asociación con la Unión Europea que habría fortalecido sus lazos políticos y económicos.

En el aniversario de esta guerra cibernética, mientras las empresas se preparaban para otra ronda de piratería, se dice que el gobierno chino pidió con éxito una retirada en el último minuto, lo que sugiere que los piratas informáticos chinos pueden compartir un mayor grado de coordinación que sus contrapartes estadounidenses (Hess, 2002).

Alcances operacionales y estratégicos de la Inteligencia militar

Internet está cambiando gran parte de la vida tal como la conocemos, para incluir la naturaleza y la conducción de la guerra. A veces, las herramientas y tácticas cibernéticas favorecerán a las naciones robustas en tecnología de la información, pero internet es una herramienta prodigiosa, que puede ser aprovechada por un grupo menor o débil para atacar a un enemigo convencional más fuerte. Al igual que con el terrorismo y las armas de destrucción masiva, la naturaleza dinámica, asimétrica y aún en evolución de los ataques cibernéticos hace que todos los aspectos de la defensa cibernética, incluida la detección, el análisis, la investigación, el enjuiciamiento, las represalias y más, sean cuestionados por los planificadores de la seguridad y la defensa nacionales.

Ahora bien, como se ha observado en los estudios de caso, es más que evidente el hecho de que los alcances operacionales y estratégicos de la Inteligencia militar se puedan beneficiar significativamente mediante el uso de herramientas cibernéticas para cumplir los objetivos planteados. No cabe la menor duda de que su potencial debe ser explorado desde una perspectiva de seguridad y defensa nacionales, ajustado a las leyes nacionales e internacionales.

Por lo tanto, analizar, diseñar, desarrollar, probar y utilizar armas cibernéticas en el futuro próximo son acciones que determinan el nuevo paso de la evolución de la guerra en el ciberespacio. Se debe agregar que los niveles estratégicos y operacionales de la Inteligencia militar deberán trabajar de la mano para proveer los recursos, métodos, técnicas, tácticas y procedimientos para el cumplimiento de las misiones de inteligencia del futuro.

Con todo y lo anterior, no se debe olvidar que los escenarios contemporáneos de la guerra tienen límites y zonas grises que deben ser tenidos en cuenta.

Escenarios contemporáneos de guerra

Patrikarakos (2021) afirma que el conflicto se aborda con dos principios rectores: en primer lugar, que la fuerza no es necesariamente el modo más apropiado para lograr los objetivos estratégicos y, en segundo lugar, que los paradigmas geopolíticos y de seguridad del siglo XX son inadecuados para dar cuenta de las amenazas contemporáneas. Por esta razón, la utilización del ciberespacio como un nuevo escenario o campo de batalla determina en muchos aspectos el efecto diferenciador en el cual los objetivos se deben alcanzar.

Al llegar a este punto, cabe indicar que existen muchas razones para determinar que los escenarios contemporáneos de la guerra están supeditados a los dominios de la guerra. La esfera del conocimiento, la influencia o actividad, el territorio sobre el cual se ejerce el dominio se convierten en unas herramientas útiles que ayudan a la descripción de áreas generales de comprensión y a la visualización y caracterización del ambiente en el que suceden las operaciones (Ejército Nacional de Colombia, 2017b).

Por lo tanto, y teniendo en cuenta que “el ciberespacio es un dominio global dentro del ambiente de la información consistente en redes interdependientes de infraestructura de tecnologías de la información y datos contenidos que incluyen: internet, telecomunicaciones, redes, sistemas informáticos y procesadores y controladores integrados” (Ejército Nacional de Colombia, 2017b, p. 491), cabe resaltar su importancia en los conflictos modernos y, por lo tanto, debe ser explotado a su máxima capacidad para generar una ventaja estratégica contra el adversario.

Conflictos de zona gris

Las leyes nacionales e internacionales no les permiten actuar de forma irracional o ilegal a las instituciones de seguridad y defensa, por lo tanto estas zonas grises son aprovechadas significativamente por las amenazas. Es decir que los lugares, áreas y actividades ilícitas que se llevan a cabo cuentan con varios respaldos importantes, entre ellos la clandestinidad, la encriptabilidad, el refugio geográfico y los vacíos de la ley.

Al respecto conviene decir que la clandestinidad permite a los actores considerados como amenazas desarrollar acciones sin determinar quiénes son y, en algunos casos, tampoco se logra saber por qué ejecutan sus planes. Además, se encuentra la encriptabilidad, la cual perfecciona a la primera debido a que dificulta la identificación forense de la red criminal. Por su parte, el refugio geográfico favorece los actos criminales de los cibercriminales, en la medida en que cuentan con

la protección de otros Estados. Finalmente, los vacíos en la ley son la base principal de la ciberseguridad y la ciberdefensa, lo cual significa que si no se cuenta con las herramientas suficientes, no se podrá generar una respuesta significativa en contra de las amenazas.

Conclusiones

Los estrategas deben ser conscientes de que parte de todo conflicto político y militar tendrá lugar en internet, cuyas características ubicuas e impredecibles hacen que las batallas que allí se libran puedan ser tan importante, si no más, que los acontecimientos que tienen lugar sobre el campo de batalla real.

Los estudio de caso sugieren que ya no se trata de tan solo piratas informáticos que tomaron por sorpresa a los planificadores de seguridad y defensa nacionales, sino que son estructuras, organizaciones y Estados mucho más complejos que deben ser estudiados desde una perspectiva más amplia.

La dinámica de la guerra contemporánea cambió gracias al dominio ciberespacial, por lo tanto, la nación que no se comprometa, hoy por hoy, en fortalecer sus medidas de ciberseguridad y ciberdefensa está caminando en una cuerda floja, literalmente, sujeta parcialmente por los dominios terrestres, marítimos, aéreos y espaciales. Es decir, no serían competidores adecuados para enfrentar las amenazas cibernéticas.

Además, la ubicuidad de los riesgos y las amenazas en el ciberespacio hacen necesario activar la ciberinteligencia en los niveles estratégicos, operacionales y tácticos, de manera que representen el camino a la categorización, la catalogación y la identificación plena de los adversarios en la guerra cibernética.

Nada puede impedir que las naciones o Estados desarrollen capacidades cibernéticas funcionales, pero el ingenio, la pericia y el conocimiento son fundamentales para conseguir el éxito en las operaciones en el ciberespacio. Asimismo, conocer la situación general, la estructura del ambiente operacional y la identificación del problema permite construir opciones en el arte operacional que favorezcan la mejor toma de decisiones en el campo de batalla.

Referencias

- BBC. (2000, 3 de noviembre). Israel Lobby Group Hakend. <https://tinyurl.com/muukxy4p>
- Bullough, O. (2002, 14 de noviembre). Russians wage cyber war on Chechen websites. <https://tinyurl.com/44h6c2vt>
- Colom, P., Coz, J., Fojón, E., & Hernández, A. (2013). Las cibercélulas: Una capacidad para la ciberseguridad y la ciberdefensa nacionales. *ARI*, (26), 1-10. <https://tinyurl.com/2p-8puuvv>
- Ejército Nacional de Colombia. (2017a). *Manual Fundamental de Referencia del Ejército MFRE 1-01 Doctrina [Público]*. Imprenta Ejército. <https://tinyurl.com/2vpdpwpm>
- Ejército Nacional de Colombia. (2017b). *Manual Fundamental de Referencia del Ejército MFRE 3-0 Operaciones [Público]*. Imprenta Ejército. <https://tinyurl.com/duc7tje>
- Ejército Nacional de Colombia. (2019). *Manual de Técnicas del Ejército MTE 5-01 Metodología de Diseño del Ejército [Público]*. Imprenta Ejército. <https://tinyurl.com/3zjfspr2>
- Geers, K. (2004, 4 de abril). Cyber Jihad and the globalization of warfare: Computer networks as a battle ground in the Middle East and beyond [Presentación en diapositivas]. <https://tinyurl.com/yjabbbox>
- Geers, K. (2009). Cyberspace and the changing nature of warfare [Keynote Speech IST-076/RSY-017]. OTAN. <https://tinyurl.com/bddy3pa>
- Geers, K. (2020). #Cyberwar: International Conflict in Cyberspace. En *Alliance Power for Cybersecurity* (pp. 3-5). Atlantic Council. <https://tinyurl.com/y5p2pajx>
- Goble, P. (1999, 9 de octubre). Russia: Analysis from Washington – A real battle on the virtual front. <https://tinyurl.com/5f798nju>
- Hess, P. (2002, 29 de octubre). China prevented repeat cyber-attack on US. <https://tinyurl.com/435u3bwz>
- Information Warfare Site [IWS]. (2001). The Information Warfare Site. <https://tinyurl.com/yyczbxu2>
- Ministerio de Defensa Nacional. (2018). *Plan Estratégico del Sector Defensa y Seguridad. Guía de Planeamiento Estratégico 2018-2022*. Ministerio de Defensa Nacional. <https://tinyurl.com/2sh6v5mt>
- Nakashima, E., & Mufson, S. (2008, 19 de enero). Hackers have attacked foreign utilities, CIA analyst says. *Washington Post*. <https://tinyurl.com/43nc2fbm>
- Organización del Tratado del Atlántico Norte [OTAN]. (1949, 4 de abril). The North Atlantic Treaty. <https://tinyurl.com/yc2ujn2t>
- Page, B. (2000, 11 de noviembre). Pro-Palestinian Hackers Threaten AT&T. *TechWeb News*. <https://tinyurl.com/5n7wnenj>
- Patrikarakos, D. (2021). *Un muy moderno “niebla de guerra”, Ucrania: siete años después*. CHARCR.

- Porteus, H. (2010, 10 de junio). *The Stuxnet Worm: ¿Just another computer attack or a game changer?* [In Brief, n.º 2010-81-E]. Parliament Information and Research Service of Canada. <https://tinyurl.com/2hu9uasw>
- Preatoni, R. (2014, 10 de agosto). Calling All Hackers. <https://tinyurl.com/29w58ryh>
- Timothy, T. (2003). Information warfare in the seconds (1999-) Chechen War: Motivator for military reform? En A. C. Aldis & R. N. McDermott (Eds.), *Russian military reform 1992-2002*. Routledge.
- Wagstaff, J. (2001, 30 de abril). The internet could be the site of the next China-US Stand-off. *The Wall Street Journal*. <https://tinyurl.com/yuk6r3j2>
- Weisman, R. (2001). California power grid hack underscores threat to U. S. news factor. <https://tinyurl.com/f7nyz54y>



Comandos

Retos de las Fuerzas Especiales e Inteligencia en la guerra contemporánea

La guerra contemporánea ofrece retos nunca vistos. Hoy en día, los ejércitos se enfrentan a adversarios más difusos, presentándose una serie de amenazas tradicionales y nuevas que se suman a entornos propios de zona gris. En este marco, las operaciones especiales y la inteligencia son protagonistas. Estas unidades altamente flexibles, adaptativas, interoperables, invisibles, con capacidades diferenciales y tecnológicas, se hacen indispensables para enfrentar a los adversarios actuales.

No obstante, se requiere repensarlas. Las capacidades críticas de las Fuerzas Especiales deben ser revisadas para evaluar nuevos medios y modos para enfrentar estos retos. De igual forma, la inteligencia debe responder a entornos cada vez más globales, de forma que la inteligencia táctica y operacional se cruza con la estratégica. Es así como la inteligencia y las Fuerzas Especiales deben trabajar en una simbiosis más profunda que la tradicional, casi borrando la frontera de lo uno y lo otro.

En el presente libro se plantean algunos debates contemporáneos y de impacto sobre el empleo de las Fuerzas Especiales y la Inteligencia en las guerras actuales. El cual es el resultado de cuatro años de reflexión académica y de investigación del Departamento Ejército de la Escuela Superior de Guerra "General Rafael Reyes Prieto". Estos aportes son pertinentes dada la especificidad del tema y los pocos estudios existentes en la academia sobre las Operaciones Especiales.



ISBN 978-628-7602-79-3

