

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? Euroinova 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>