

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/bdzjhjvdy>
- 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/rldt.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/mu2vbmu6>
- 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>