Estudio acerca de la importancia y necesidad de formar personal calificado en la FAC, para la implementación, desarrollo y conduccion de operaciones en el ciberespacio, como una estrategia miliar

Jaime Ramirez Aguirre

Trabajo de grado para optar al título profesional:

Curso de Estado Mayor (CEM)

Escuela Superior de Guerra "General Rafael Reyes Prieto"
Bogotá D.C., Colombia

2013

FUERZAS MILITARES DE COLOMBIA

ESCUELA SUPERIOR DE GUERRA

ESTUDIO ACERCA DE LA IMPORTANCIA Y NECESIDAD DE FORMAR PERSONAL CALIFICADO EN LA FAC, PARA LA IMPLEMENTACIÓN, DESARROLLO Y CONDUCCIÓN DE OPERACIONES EN EL CIBERESPACIO, COMO UNA ESTRATEGIA MILITAR.

MY. FAC RAMIREZ AGUIRRE JAIME

Curso CEM-13

Bogotá DC

Noviembre del 2013

FUERZAS MILITARES DE COLOMBIA

ESCUELA SUPERIOR DE GUERRA

TRABAJO DE GRADO PRESENTADO PARA OPTAR EL TITULO DE ESTADO MAYOR, CEM 2013.

ESTUDIO ACERCA DE LA IMPORTANCIA Y NECESIDAD DE FORMAR PERSONAL CALIFICADO EN LA FAC, PARA LA IMPLEMENTACIÓN, DESARROLLO Y CONDUCCIÓN DE OPERACIONES EN EL CIBERESPACIO, COMO UNA ESTRATEGIA MILITAR.

MY. FAC RAMIREZ AGUIRRE JAIME

Curso CEM-13

Bogotá DC

Noviembre del 2013

aceptación

Este proyecto está dedicado a Dios, por permitirnos disfrutar de la vida día tras día. A mi esposa e hijas, por acompañarme incondicionalmente a lo largo de la vida y carrera militar. A la Fuerza Aérea Colombiana y todos los entes cooperadores, por las oportunidades brindadas a lo largo de nuestra carrera profesional y militar; lo cual ha permitido encontrar el rumbo, que me llena de experiencias significativas y motivan a querer aportar lo mejor de nuestras capacidades en pro del desarrollo de la fuerza.

AGRADECIMIENTOS

Es un placer agradecer a todas y cada una de las personas que hicieron posible la realización de este trabajo.

A Dios por poner en nuestro camino a quienes guiaron el desarrollo de este proyecto. ……..

RESPONSABILIDAD AUTORES

El contenido de este documento corresponde exclusivamente al pensamiento de los autores y es de su absoluta responsabilidad. Las posturas y aseveraciones aquí presentadas son resultado de un ejercicio académico que no representa la posición oficial, ni institucional de la Escuela Superior de Guerra, de las Fuerzas Militares o del Estado colombiano.

GLOSARIO

AMENAZA: la posibilidad de compromiso, pérdida o robo de información clasificada o de servicios y recursos que la soportan. Una amenaza puede ser definida por su origen, motivación o resultado y puede ser deliberada o accidental, violenta o subrepticia, externa o interna. [1]

ASPIRANTES A OFICIALES: son los alumnos de la Escuela de Formación Marco Fidel Suarez, EMAVI.

CIBERESPACIO: El mundo digital generado por ordenadores y redes de ordenadores, en el cual personas y ordenadores coexisten y el cual incluye todos los aspectos de la actividad "online".[2]

CIBERGUERRA: es el desplazamiento de un conflicto, en principio de carácter bélico, que toma el ciberespacio y las tecnologías de la información como escenario principal, en lugar de los campos de batalla convencionales.[3]

CIBERATAQUE: Forma de ciberguerra / ciberterrorismo donde combinado con un ataque físico o no se intenta impedir el empleo de los sistemas de información del adversario o el acceso la misma.[4]

---

[1] MINISTERIO DE DEFENSA. Ciberseguridad. Madrid, Instituto español de estudios estratégicos. 2011. p.347

[2] Ibid., p.348

[3] ESCUELA SUPERIOR DE GUERRA, Cr DEYSI GARCES. Ciberguerra. Bogotá, CEM. 2013

[4] MINISTERIO DE DEFENSA. Ciberseguridad. Op Cit., p.348

CIBERDEFENSA: La aplicación de medidas de seguridad para proteger las los diferentes componentes de los sistemas de información y comunicaciones de un ciberataque.[5]

CIBERGUERRERO: Persona cualificada y con un amplio dominio del ciberespacio.[6]

CIBERSEGURIDAD: Protección de los componentes de las infraestructuras de los sistemas de información y comunicaciones ante amenazas cibernéticas.[7]

EXPERTO EN PERIMETRAL: persona con amplio conocimiento del terreno en el ciberespacio.

EXPERTO EN VIROLOGÍA: persona con amplio conocimiento en virus, que circulan a través del ciberespacio.

EXPERTO EN CONTINGENCIA: persona con amplio conocimiento, para ejecutar planes de acción de defensa o ataque a través del ciberespacio.

EXPERTO EN INTRUSIÓN: personas con amplio conocimiento, para penetrar información a través del ciberespacio.

FORMACIÓN ACADÉMICA: o profesional desarrolla las habilidades necesarias en el futuro oficial que lo hagan competente tanto en el *ser* (actitudes y valores, relacionados con resultados de tipo axiológicos), en el *hacer* (procedimientos relacionados con resultados de tipo cognitivo y motriz) y en al *conocer* (conceptos

---

[5] Ibid., p. 348
[6] Ibid., p.348
[7] Ibid., p. 348

teorías, principios, hechos, relacionados con resultados de tipo cognitivo), para desempeñarse como profesional en las carreras que ofrece la EMAVI.

FORMACIÓN INTEGRAL: es entendida por la Escuela Militar de Aviación como la articulación armónica entre las dos áreas de formación que deben desarrollarse en el aspirante a oficial de la Fuerza Aérea Colombiana: la formación militar y la formación académica o profesional.

INNOVACIÓN EDUCATIVA: todas aquellas nuevas estrategias que permiten transmitir el conocimiento.

INNOVACIÓN TECNOLÓGICA: todas aquellas nuevas estrategias, que permiten el desarrollo de nuevas tecnologías.

INFRAESTRUCTURAS CRÍTICAS: Las infraestructuras estratégicas cuyo funcionamiento es indispensable y no permite soluciones alternativas, por lo que su interrupción o destrucción tendría un grave impacto sobre los servicios públicos esenciales.[8]

INFORMACIÓN: Conocimiento que puede ser comunicado de cualquier forma.[9]

INFRAESTRUCTURAS ESTRATÉGICAS: Las instalaciones, redes, sistemas y equipos físicos y de tecnología de la información sobre las que descansa el funcionamiento de los servicios públicos esenciales.[10]

---

[8] CARO Bejarano, Marí José. La protección de las infraestructuras críticas, Madrid. 2011. p2

[9] MINISTERIO DE DEFENSA. Ciberseguridad. Op Cit., p.348

[10] Ibid., p 348

OPERACIONES AÉREAS: "son acciones concretas que implican el uso del poder aéreo y espacial, mediante las cuales se cumplen las funciones y por ende la misión de la FAC y se logran los objetivos propuestos en los planes y órdenes Militares correspondientes".[11]

OPERACIONES EN EL CIBERESPACIO: son el conjunto de estrategias enfocadas a la protección de la vasta red de servidores, computadoras y demás aparatos, conectados entre sí, que nos permite transmitir y recibir información de todo tipo.[12]

PERSONAL CALIFICADO: personas con competencias y formación idónea en determinado campo.

PERSONAL CUALIFICADO: personas con una formación integral amplia, con cualidades y competencias específicas en un determinado campo.

SEGURIDAD NACIONAL: todas aquellas estrategias que permiten la defensa de una Nación.

---

[11] ESCUELA SUPERIOR DE GUERRA. Doctrina Aérea. Fuerzas Militares. Bogotá, CEM 2012. P. 35.
[12] MANTHORPE, William. The emerging joint system of systems. NY, 1996. p. 307

ABREVIATURAS

CID. Confidencialidad, integridad y disponibilidad.

CBS. Ciberespacio.

DD.HH. Derechos Humanos.

DICA. Derecho Internacional de los Conflictos Armados.

DIH. Derecho Internacional humanitario.

EMAVI. Escuela Militar de Aviación.

EMD. Extracción, modificación, denegación de servicio.

ESINA. Escuela de Inteligencia Aérea.

FAC. Fuerza Aérea Colombiana.

JIN. Jefatura de Inteligencia Aérea.

JOA. Jefatura de Operaciones Aéreas.

OCBS. Operaciones en el ciberespacio

INDICE

pág

LISTA DE TABLA

pág

LISTA DE GRÁFICAS

pág

LISTA DE ANEXOS

pág

RESUMEN

El propósito de este proyecto es realizar un estudio acerca de la importancia y necesidad de formar personal calificado en la FAC, para la implementación, desarrollo y conducción de operaciones en el ciberespacio, como una estrategia militar.

Con un personal teniendo una formación actualizada y oportuna en, ciberespacio, el liderazgo y la orientación de los recursos humanos y técnicos en esta área, serán mejor direccionados a la consecución de resultados positivos y certeros en la implementación y desarrollo de operaciones en el ciberespacio, lo cual hace parte de la visión de la FAC, ya que se debe fortalecer tanto ofensiva como defensivamente para los ataques cibernéticos, que trae consigo el acelerado desarrollo tecnológico y globalizado de la humanidad, contribuyendo aún más a la Seguridad Nacional, que es un objetivo primordial de la Fuerza Aérea Colombiana

Es un proyecto que tiene características de investigación y acción, donde se amplía un conocimiento, para lograr fortalecer a una Fuerza, que se enfrenta a los acelerados desarrollos tecnológicos y así ofrecer un mejor servicio, en pro de contribuir a la Seguridad Nacional.

Palabras claves: personal calificado, formar, operaciones en el ciberespacio, Seguridad Nacional, Estrategia Militar.

INTRODUCCIÓN

El propósito de este proyecto es realizar un estudio acerca de la importancia y necesidad de formar personal calificado en la FAC, para la implementación, desarrollo y conducción de las operaciones en el ciberespacio, como una estrategia militar.

Es un proyecto de tipo aplicativo cuya metodología se basa en elementos cuantitativos, ya que se trabaja sobre instrumentos medibles, como encuestas y teniendo como base los resultados se procede a realizar las entrevistas, que permiten presentar un estudio objetivo que justifica la importancia y necesidad de formar a todo el personal de la FAC, en todos los adelantos y avances en el campo del ciberespacio, para así direccionar a la fuerza en la implementación, desarrollo y conducción de operaciones en el ciberespacio.

Para la Fuerza Aérea Colombiana es fundamental la formación intelectual y técnica de sus integrantes, por ello se ha esforzado en brindar una formación integral a su personal; lo cual abarca el primer objetivo; siendo importante analizar para desarrollar este proyecto, es por eso que se identifica y analiza la formación integral impartida a los oficiales, a través de la educación militar y la educación académica de pregrado y tecnológica, contenido en el capítulo 3. El personal debe estar preparado para aprovechar al máximo los desarrollos tecnológicos propios de las ciencias aeroespaciales. Pero además el ciudadano militar debe contar con hábitos intelectuales, criterios para el respeto a las leyes y un profundo conocimiento de los avances globales, para el desarrollo de la fuerza. Todo con el objetivo de ejercer responsablemente sus actividades y desarrollar sus virtudes militares. Además capacita y entrena a sus soldados y personal no uniformado, quienes soportan el funcionamiento de la fuerza.

Cabe también resaltar, que la Escuela Superior de Guerra, a través de la Línea de Investigación en Desarrollo Científico, Tecnológico e Innovación del ESDEGUE-

SIIA-CEESEDEN, se ha interesado por analizar cuál ha sido, y será en el futuro, la incidencia del desarrollo tecnológico, en un mundo globalizado, es por ello que en abril del 2013 se presenta un proyecto que busca, que el personal militar que allí se forma tenga claridad y este actualizado, con todos los conceptos importantes, en esta campo del ciberespacio (ver anexo E).

La Fuerza Aérea Colombiana busca dentro de la formación de su personal capacitarlo en campos propios de la actividad militar, lo cual incluye el dominio del ciberespacio, aplicado a la conducción de operaciones, la cual, desarrolla el segundo objetivo, de vital importancia para el desarrollo de este proyecto, es por eso que también se identifica y analiza la capacitación del personal de la Fuerza Aérea en conocimientos que conduzcan al dominio del ciberespacio, más específicamente en operaciones en el ciberespacio, este contenido se encuentra en la segunda parte del tercer capítulo. Se debe tener claro que las operaciones en el ciberespacio hacen parte de la ciberguerra.[13] La FAC se está interesando en este campo, para ser una Fuerza a la vanguardia en cuanto a optimizar y modernizar sus operaciones, para mantener el control del espacio aéreo-espacial. Las capacitaciones en ciberespacio, para el desarrollo y conducción de las operaciones en el ciberespacio impartida al personal de la FAC, es muy escaza y está supeditada a lo que otras entidades educativas tengan para ofrecer, en dicho tema; lo cual en muchas ocasiones no llena las expectativas, para el cumplimiento de la misión.

Para la Fuerza Aérea Colombiana es de vital importancia fortalecerse en la implementación, desarrollo y conducción de operaciones en el ciberespacio , ya que le permitirá contribuir a alcanzar los objetivos primordiales de las Fuerzas Militares en pro de la Seguridad Nacional, y cumplir a cabalidad con su misión de

---

[13] MINISTERIO DE DEFENSA NACIONAL, Comando General Fuerzas Militares. Inteligencia Estratégica. Bogotá (2da Edición), 2000. p.15.

ejercer un total dominio sobre el espacio aéreo, es por esto que es relevante analizar la capacidad de las operaciones en el ciberespacio, como una estrategia militar en la FAC, lo cual, desarrolla el tercer objetivo, este contenido se encuentra en la tercera parte del tercer capítulo. La Estrategia Militar se define, según Lindell Hart [14] como el arte de distribuir y hacer actuar los medios militares para alcanzar los objetivos políticos. Y Las operaciones en el ciberespacio: Son el conjunto de estrategias enfocadas a la protección de la vasta red de servidores, computadoras y demás aparatos, conectados entre sí, que nos permite transmitir y recibir información de todo tipo. Un recuento histórico de ciberguerra o guerra a través del ciberespacio a nivel mundial, el poder aéreo-espacial, la ciberdefensa y el ciberataque ,como componentes indispensables, para conducir operaciones en el ciberespacio, los elementos y características del ciberespacio, al igual que un análisis de la infraestructura crítica, sus amenazas, capacidades de otros países y las capacidades de Colombia para enfrentar la amenaza CONPES, así como los aviones no tripulados, los cuales pueden llegar a ser vulnerables a un ciberataque; hacen parte de este capítulo, lo que permite entender la importancia de formar personal calificado o mejor aún cualificado, para implementar, desarrollar y conducir operaciones en el ciberespacios, como una estrategia militar.

Es muy importante para el desarrollo de este proyecto analizar la visión y misión institucional, así como todas las leyes que se deben tener en cuenta en este campo del ciberespacio y la conducción de operaciones, contenido en el cuarto capítulo. Para una Institución Militar, como es la Fuerza Aérea Colombiana, el dominio de todos los temas que tiene que ver con la ciberguerra y en especial con las operaciones en el ciberespacio, son de gran relevancia; ya que permiten liderar y direccionar mejor los recursos en los procesos que abarcan este campo del ciberespacio, contribuyendo a implementar, desarrollar y conducir las

[14]Ibid., p. 14.

operaciones en el ciberespacio, en pro de la Seguridad Nacional y del derecho internacional humanitario.

Los materiales y métodos, contenidos en el quinto capítulo, que se utilizaran para el desarrollo de este proyecto, abarcan: el enfoque, ya que es necesario enfocar el proyecto en varias etapas o fases para asegurar que el estudio que justifica la propuesta, sea acorde a las necesidades de la FAC y al servicio educativo que se ofrece; la estrategia y su procedimiento en la investigación se dará a través de la recolección y análisis de información, de acuerdo al orden de los objetivos planteados, utilizando la encuesta como un instrumento, lo que permitió ir paso a paso y no desviar el estudio propuesto y el procesamiento de la información se realizó a través de la tabulación de un análisis de frecuencia de los resultados y sus respectivas gráficas, las cuales permitieron realizar una análisis de los resultados, concretando la viabilidad en cuanto a importancia , necesidad e interés del proyecto de investigación.

En las conclusiones y recomendaciones se plantea la importancia y necesidad de formar personal calificado en la FAC, para la implementación, desarrollo y conducción de operaciones en el ciberespacio, como una estrategia militar a través de la innovación tecnológica y educativa, evidenciando el cumplimiento de los objetivos propuestos en este proyecto y dando solución al problema planteado; con las respectivas alternativas.

A través de este proyecto se quiere mostrar la necesidad e importancia de formar personal calificado, para la implementación, desarrollo y conducción de las operaciones en el ciberespacio, desarrollando el cuarto objetivo, se alcanza la meta, de lo importante y necesario que es, dar a conocer las innovaciones tecnológicas y educativas, de forma oportuna, para así optimizar y contribuir en este campo tan importante de las operaciones en el ciberespacio, lo que permite hacer frente a este mundo globalizado. Lo cual va acorde con la visión que establece, que la "Fuerza Aérea del futuro sea una organización militar con

participación decisiva en la defensa de la nación, con hombres y mujeres que aporten lo mejor de su talento y experiencia, para el cumplimiento de la misión asignada".[15]

[15] FUERZA AÉREA COLOMBIANA. Vocación de victoria. Bogotá, 2005. p. 52.

1 JUSTIFICACIÓN

La Fuerza Aérea Colombiana mantiene dentro de sus políticas desarrollar operaciones aéreas oportunas, pensando siempre en estar a la vanguardia para el dominio del espacio aéreo, es por ello que es de vital importancia formar personal calificado en la implementación, desarrollo y conducción de operaciones en el ciberespacio, como una estrategia militar. Ayudando así al desarrollo de la fuerza de forma proactiva y asertiva, para la toma de decisiones por parte de los comandantes.

A través de los tiempos la humanidad ha comenzado a librar guerras en su ámbito natural, es así como se desarrollaron los ejércitos y la forma de derrotar al enemigo el cual se encuentra también en un ámbito terrestre. A medida que el ser humano ha necesitado sobrevivir ante su oponente, ha tenido que migrar a otros ámbitos como el marítimo y el aéreo a principios del siglo XX.

A finales del siglo XX el desarrollo de la tecnología nos ha llevado a crear un nuevo ámbito de la guerra el "cibernético" en el cual a diferencia de los otros teatros de operación donde se transporta materia o energía, en este se transportan y utilizan datos, conocimiento e información.

La ciberguerra o guerra a través del ciberespacio, afecta a la Fuerza en la necesidad de sobrevivir en este ámbito en contra de sus oponentes. Es imperativo que la Fuerza Aérea, fortalezca sus sistemas tanto administrativos como operativos, en los niveles estratégico, operativo o táctico, que permita proteger sus capacidades distintivas dentro del marco del conflicto, sobre todo en donde en la actualidad la institución ha incrementado y mejorado la capacidad operativa, poniendo a la institución en una condición sobresaliente con respecto a las demás fuerzas aéreas del continente.

En Colombia hay demasiados oponentes al Estado los cuales pueden llegar a afectar la infraestructura y el normal funcionamiento de los sistemas. En la actualidad, Colombia ha iniciado un proceso de estructuración en el fortalecimiento de sus capacidades de identificación, análisis y estudio de cursos de acción que protejan al país de amenazas o ataques de este tipo que puedan conducir a determinados sectores a vivir y sufrir una crisis por consecuencia de los ataques a que somos objeto.

Es crucial determinar cursos de acción y toma de decisiones basadas en experiencias actuales de otros países que han sido afectados por este tipo de amenaza, y que a la postre ponen en riesgo la seguridad de una nación y por ende sus objetivos nacionales.

Es importante que la Fuerza Aérea tome las acciones necesarias para enfrentar los avances tecnológicos y globalizados de la humanidad y así pueda implementar, desarrollar y conducir operaciones en el ciberespacio, como una estrategia milita. Se deben formular preguntas sobre posibles situaciones que afecten el normal funcionamiento y estructura de una organización; se plantea el supuesto de un bloqueo en el sistema de nominas en guerra regular con otro país ¿cuál sería el efecto en la moral de las tropas? ¿Cómo afectaría esa gran cadena financiera en la cual se debe recibir y entregar información a la vez?, Se debe pensar en todas las amenazas existentes que se encuentran en el ciberespacio.

Es claro que con personal calificado en la implementación, desarrollo y conducción de operaciones en el ciberespacio se potencializan las capacidades de la jefatura de operaciones aéreas, la Jefatura de Inteligencia y jefatura de apoyo logístico, específicamente DITIN(dirección tecnología de la información); ya que se tendrían oficiales capaces de liderar y direccionar los recursos humanos y técnicos en esta área, así la FAC cumpliría a cabalidad con su misión, contribuyendo de forma certera en la Seguridad Nacional y el derecho internacional humanitario.

2 PLANTEAMIENTO DEL PROBLEMA

Durante los últimos años, la Fuerza Aérea Colombiana ha querido hacer uso del ciberespacio, aplicado al manejo, desarrollo y conducción de las operaciones, lo cual ha intentado, capacitando a su personal, ya sea a nivel nacional o internacional; pero estos esfuerzos no han sido suficientes, ya que el personal que maneja los avances en ciberespacio es muy escaso y son pocos los comandantes que tienen las competencias en este campo, necesarias para direccionar y liderar con una visión clara y objetiva, perdiendo así la oportunidad de estar a la vanguardia en el desarrollo de operaciones en el ciberespacio, en pro de la Seguridad Nacional.

La historia de internet se remonta al desarrollo de las redes de comunicación que fueron diseñadas para permitir la comunicación general entre usuarios de varias computadoras. Estas ideas aparecieron a finales de los años cincuenta pero su implementación práctica se empezó a finales de los ochenta y a lo largo de los noventa. En la década de 1980, se reconoció lo que conocemos como Internet y a partir de los 90 se expandió por el mundo el término de ampliar la red mundial.

> *"La infraestructura de Internet se esparció por el mundo, para crear la moderna red mundial de computadoras que hoy conocemos. Atravesó los países occidentales e intentó una penetración en los países en desarrollo, creando un acceso mundial a información y comunicación sin precedentes, pero también una brecha digital en el*

acceso a esta nueva infraestructura. Internet también alteró la economía del mundo entero, incluyendo las implicaciones económicas[16].

En este sentido, partiendo del principio en el cual la ciberguerra se traduce como una guerra de control, y que adicionalmente existe a través de diversas armas cibernéticas que se desenvuelven y generan sus impactos en un mundo virtual que trasciende a los escenarios físico, el fenómeno de la guerra cibernética en la actualidad hace referencia explícita a:

> "Una agresión promovida por un Estado y dirigida a dañar gravemente las capacidades de otro para tratar de imponerle la aceptación de un objetivo propio o, simplemente, para sustraerle información, cortar o destruir sus sistemas de comunicación, alterar sus bases de datos, es decir, lo que habitualmente se entiende como guerra, pero con la diferencia de que el medio empleado no sería la violencia física, sino un ataque informático que le permita obtener una ventaja sobre el enemigo para situarse en superioridad, o incluso derrocarle"17

Un adecuado dominio del ciberespacio, permite contrarresta los actos criminales cibernéticos que tienen la capacidad de interrumpir los servicios de mantenimiento de la vida, causar catastróficos daños económicos, o degradar severamente las redes de las cuales depende la Defensa Nacional y las Agencias de Inteligencia.

En el año 2012 en Colombia se recibieron ataques de una red llamada BotNet Mariposa, y para el 2011 el grupo "hacktivista" Anonymous atacó los portales de la Presidencia de la República, el Senado, Gobierno en Línea y los Ministerios del Interior y Justicia, Cultura y Defensa, dejándolos fuera de servicio por varias horas; motivo por el cual este tema hacer parte de la agenda nacional.

---

[16] Historia del Internet [En línea] Disponible en: http://ciberespacio-total.blogcindario.com/2010/09/00001-ciberespacio-historia-del-internet-glosario-relacionado-al-tema-otros-etc-actividad-n-1.html Citado el 22 de marzo de 2012

[17] SANCHEZ Medero, Gema. En: Revista Política y Estrategia N° 114 – 2009.p20.

Dentro de la evolución de las guerras y los conflictos se debe partir del principio que la guerra y la política siempre estarán ligadas, serán entonces el resultado del desafío continuo a las lealtades políticas y sociales a las causas, más que a la nación. Estarán marcadas por el incremento del poder de las pequeñas células y el desarrollo descontrolado de la tecnología, por ello las Fuerzas Militares de Colombia deben prepararse para la extensión de la guerra asimétrica e insurgente, donde el enemigo utiliza todos los medios - las tácticas militares convencionales y no convencionales y armas a la cual se incluye causas políticas, religiosas y sociales; incorpora las campañas estratégicas globales de las operaciones de información (Internet y el ciclo de 24 horas de las noticias); siendo conducida ya sea por organizaciones al margen de la ley o por organizaciones sociales con el propósito de interrumpir y derrotar enemigos superiores para alcanzar la toma del poder.

Es por ello que es de vital importancia para direccionar, liderar y orientar la implementación, desarrollo y conducción de operaciones en el ciberespacio, formar personal calificado en innovaciones tecnológicas y educativas de cibernética, si se quiere una fuerza fortalecida y preparada para el acelerado desarrollo tecnológico y globalizado de la humanidad, como estrategia militar, en pro la Seguridad Nacional.

2.1 FORMULACIÓN DEL PROBLEMA

¿Por qué es importante formar personal calificado en la FAC, para la implementación, desarrollo y conducción de las operaciones en el ciberespacio?

2.2 OBJETIVO GENERAL

Realizar un estudio acerca de la importancia y necesidad de formar personal calificado en la FAC, para la implementación, desarrollo y conducción de

operaciones en el ciberespacio, como estrategia militar, en pro de la Seguridad Nacional.

2.3 OBJETIVOS ESPECÍFICOS

2.3.1 Identificar los antecedentes de formación integral a los oficiales, a través de la educación profesional militar y la educación académica impartida en la Fuerza Aérea Colombiana.

2.3.2 Analizar los antecedentes y el contexto de la capacitación del personal de la FAC, en conocimientos que permitan el dominio del ciberespacio, para la implementación, desarrollo y conducción de operaciones en él.

2.3.3 Evaluar la importancia de una adecuada y pertinente formación, enmarcada en ciberespacio, para potencializar la capacidad de las operaciones en el ciberespacio, como una Estrategia Militar.

2.3.4 Analizar la importancia y necesidad de formar personal calificado en la FAC para la implementación, desarrollo y conducción de las operaciones en el ciberespacio.

3 DESARROLLO DE CONCEPTOS

3.1 FORMACIÓN INTEGRAL AL PERSONAL, A TRAVÉS DE LA EDUCACIÓN MILITAR Y LA EDUCACIÓN ACADÉMICA EN LA FAC.

Para la Fuerza Aérea Colombiana es fundamental la formación intelectual y técnica de sus integrantes, por ello se ha esforzado en brindar una formación integral a los oficiales y suboficiales. "El personal debe estar preparado para aprovechar al máximo los desarrollos tecnológicos propios de las ciencias aeroespaciales; además, el ciudadano militar debe contar con hábitos intelectuales, criterios para el respeto a las leyes y un profundo conocimiento de su especialidad"[18]; todo con el objetivo de ejercer responsablemente sus actividades y desarrollar sus virtudes militares. Así mismo, capacita y entrena a sus soldados y personal no uniformado, quienes soportan el funcionamiento de la fuerza.

Jefatura de Educación Aeronáutica, JEA

La FAC busca constantemente modernizar y actualizar los procesos de formación, capacitación, instrucción y entrenamiento, para así potencializar las competencias requeridas en el cumplimiento de su misión institucional. Para ello, creo la Jefatura de Instrucción y Entrenamiento, JIE, mediante disposición 007 del 23 de febrero de 1996; la cual es la encargada de centralizar las actividades educativas de la fuerza, que hasta entonces estaban repartidas entre la dirección de la institución y entrenamiento de vuelo, DINEV, orgánica de la jefatura de Operaciones Aéreas, que dirigía los procesos de instrucción y entrenamiento de vuelo y las escuelas de formación y capacitación, de otras dependencias. Mediante la disposición 003 de

---

[18] Ibid., p. 6.5

2001 se le cambio la denominación por la de Jefatura de Educación Aeronáutica. Bajo su responsabilidad quedo el área funcional de Educación, Ciencia y Tecnología, a través de las direcciones de educación superior, instrucción y entrenamiento, Certificación y Acreditación, y Ciencia y Tecnología. Así mismo, de la jefatura dependen funcionalmente los grupos académicos de las escuelas de formación, el Instituto Militar Aeronáutico de las unidades.

En 2004, se creó la Dirección de Doctrina Aeroespacial; de acuerdo a lo anterior, "la misión de esta jefatura es planear, dirigir y supervisar la ejecución de los planes y programas de formación, capacitación, instrucción, y entrenamiento, así como, generar la Doctrina Aeroespacial y orientar el desarrollo de la ciencia y tecnología en la Fuerza Aérea", [19] con el fin de fortalecer y facilitar la conducción y ejecución de las operaciones aéreas; en acciones coordinadas con la Jefatura de Seguridad y Defensa de Bases Aéreas.

Escuela Militar de Aviación Marco Fidel Suarez, EMAVI.

"*La misión de la Escuela Militar de Aviación es formar integralmente a los futuros Oficiales de la FAC para conducir operaciones aéreas que permitan derrotar al enemigo y ejercer Soberanía Nacional*"; [20] para optimizar esta tarea, los programas se actualizan de forma permanente, lo mismo que las técnicas y conocimientos aeronáuticos. La intensa preparación militar y académica responde a los requerimientos que el oficial de la Fuerza Aérea debe asumir desde su desempeño profesional, y se traduce en mejor empleo de los recursos asignados a la Fuerza Aérea, y en mayor agilidad y eficiencia para atender sus responsabilidades operativas.

---

[19] Ibid., p. 66,67.
[20] Ibid., p. 67.

"En Colombia nació la primera Escuela Militar de Aviación en la población de Flandes, Tolima, en 1921. Fue creada por el decreto 2257 de ese año, con el objeto de formar Pilotos Militares y Mecánicos de la Aviación; la cual funciono hasta mayo de 1922, pero fue reabierta el 8 de noviembre de 1924 en Madrid, Cundinamarca". [21] Este acontecimiento considerado, de gran importancia fue la fecha escogida para celebrar el aniversario de la FAC. Ya en 1933, la escuela fue trasladada a la hacienda El Guavito en Cali, Valle del Cauca, donde funciona hoy; adoptando el nombre de Marco Fidel Suarez, en honor al señor Presidente que creó la aviación militar en Colombia.

3.1.1.1 Evolución de los programas académicos.

El fortalecimiento del área académica en EMAVI, hace parte de su devenir histórico. Durante un tiempo los Cadetes adelantaban estudios universitarios en ingeniería o en Economía pero circunstancias de orden institucional hicieron que se suspendieran, retomando el énfasis en la formación militar y de vuelo.[22]

A finales de los años setenta, el crecimiento de la fuerza y la necesidad de administrar en forma adecuada sus valiosos recursos, reorientaron el proyecto educativo de la Escuela hacia la formación académica con énfasis en administración. EMAVI, inició en firme el proceso cuando recibió la aprobación para adelantar el programa de Administración Aeronáutica. El Instituto Colombiano para el fomento de la educación Superior, ICFES, expidió para ello la resolución 571 del 19 de marzo de 1992, y como consecuencia, el tiempo de formación de los oficiales aumento de tres a cuatro años. El primer curso de esta modalidad fue el No. 69. Los oficiales de los cursos No 54 al No 68, quienes habían adelantado seis

---

[21] ECHAVARRIA Barrientos, Raúl. En la Ruta de las Estrellas, Libro de oro, EMAVI. Cali 1983. p. 67.
[22] Ibid., p. 67.

semestres de administración Aeronáutica en EMAVI, finalizaron sus estudios para obtener el título profesional durante los cursos para ascenso en el IMA.

"*Basados en los planes Estratégicos de la Fuerza, la Escuela creó el programa de pregrado de Ingeniería Mecánica, aprobado en diciembre del 2000, ello con el objetivo de afianzar el liderazgo en el sector aeronáutico nacional. La primera promoción fue el curso No 77 A. El programa de Ingeniería Informática (ver anexo C) fue aprobado octubre del 2002, y su primera promoción el curso No 79 C*". [23]

Estos nuevos desafíos llevaron a postergar, para el primer año de oficiales, la realización de las especialidades militares (Vuelo, Defensa Aérea, Comunicaciones, Navegación, Mantenimiento, Abastecimientos, Armamento Aéreo, y Seguridad y Defensa de Bases). No era para menos, pues la Escuela estaba empeñada en conseguir la acreditación; por parte del Consejo Nacional de Acreditación CNA, y el cumplimiento de otras exigencias del Sistema Educativo Nacional, como los estándares de calidad en aspectos relativos a la implementación del sistema de créditos, los exámenes de Calidad para la Educación Superior, ECAES, y la obtención del llamado Registro calificado. En pro de esta búsqueda de la calidad y mejoramiento se creó el Centro de Investigación y Tecnología Aeronáutica, CITA.

La FAC ha cambiado su sistema educativo. En la actualidad, gradúa Oficiales en las carreras de Administración Aeronáutica, Ingeniería Mecánica o Ingeniería Informática. La capacitación como pilotos se realiza una vez el alumno ha ascendido al grado de Subteniente, es decir, en su quinto año en la institución, se ha creado un *Guavito Virtual* donde se realizan simulaciones de vuelo en diferentes aviones y helicópteros militares y formación de aeronaves. Además, el alumno participa en las fases de planeación de una operación aérea: análisis de

---

[23] Ibid., p. 69

inteligencia militar técnica, entrega de armamento, apoyo aerotáctico, evacuaciones aeromédicas, y otras relacionadas con la aplicación de la Fuerza. Familiarizándose, así con los conocimientos que aplicaran durante la etapa de formación como pilotos militares. Además la Fuerza Aérea tiene el proyecto de convertir la escuela militar de aviación en "Universidad del Aire". Para ello, se pondrán en marcha otras carreras como: Ingeniería Electrónica e Ingeniería Aeronáutica inicialmente. Todo con el objetivo de hacer realidad el lema del Alma Mater: *La ciencia mi ruta, mi meta el espacio*. "La Universidad del Aire estará conformada además, por una facultad Tecnológica a cargo de la Escuela de Suboficiales y una facultad de Posgrados a cargo del Instituto Militar Aeronáutico".[24]

"*Los oficiales de la FAC están distribuidos en: Cuerpo de Vuelo, Cuerpo Logístico, Cuerpo de Seguridad y Defensa de Bases Aéreas, Cuerpo Administrativo y Cuerpo de Justicia Penal Militar*". [25] Esta distribución permite tener una visión más concreta y amplia de las especialidades existentes legalmente. El Cuerpo de Vuelo está compuesto por las especialidades de Pilotaje, Navegación, Inteligencia Técnica Aérea y defensa Aérea, la cual nació como resultado de la instalación y operación de radares. En este lapso también creció el número de navegantes debido al aumento de equipos de Inteligencia y de reconocimiento a bordo de las aeronaves. El Cuerpo de Seguridad y Defensa de Bases Aéreas antes denominado Infantería de Aviación, conformado por las especialidades de Inteligencia y Defensa de Bases Aéreas.

Instituto Militar Aeronáutico, IMA

---

[24]Ibid., p. 70, 71.
[25]FUERZA AÉREA COLOMBIANA. Vocación de victoria. Bogotá.2009, p. 83

El IMA tiene la misión de formar y capacitar integralmente al personal de Oficiales de la Fuerza Aérea en el desarrollo de su carrera militar, para proporcionarles una formación optima que les permita ejercer adecuadamente el liderazgo del Poder Aéreo Nacional. "La ley 126 de 1959 y su Decreto orgánico reglamentaron la carrera de oficiales y suboficiales, esas normas establecieron que quienes quisieran ascender a los grados de Capitán y Mayor debía, como requisito previo, tomar y aprobar un curso de capacitación".[26] En consecuencia, mediante disposición 16 del 07 de abril de 1960, fue creado el Instituto Militar Aeronáutico y se aprobó la Tabla de Organización y Dotación. Sus primeras instalaciones se ubicaron en el Aeropuerto de Techo, donde funciono hasta julio de 1971, la fecha en la cual fue desactivado y sus cursos agregados a los dictados por la Escuela Militar de Aviación.

Ya en mayo de 1982, los cursos de capacitación y comando fueron trasladados al recién creado Instituto de capacitación de oficiales, ICAPO, con sede en las instalaciones de la Base Aérea BG. (h) Camilo Daza Álvarez, en el aeropuerto El Dorado de Bogotá. Al ano siguiente, fue adoptada de nuevo la denominación Instituto Militar Aeronáutico, IMA. El ICFES, mediante resolución 571 de 1992 certifico a IMA y a EMAVI para expedir el título de Administrador Aeronáutico a los Oficiales de la Fuerza Aérea. En diciembre de 1994, el IMA se trasladó a las instalaciones de la Escuela Superior de Guerra, en el Canton Norte de Bogotá, donde funciona actualmente. Con el tiempo surgió la necesidad de ofrecer programas de posgrado a los oficiales graduados como Administradores Aeronáuticos en EMAVI o en otros programas de pregrado por convenios con universidades. Esta necesidad llevo a definir un nuevo papel para IMA.

---

[26]Ibid., p. 72.

"*La Ley 30 de 1992, estableció un régimen especial para las Escuelas de la Fuerza Aérea*", [27] en consecuencia, se iniciaron los trámites para acreditar al IMA como Unidad de posgrados y se logró la admisión del Instituto a la Asociación Colombiana de Facultades de Administración, ASCOLFA. En 1999, suscribió un convenio técnico- Educativo con la Universidad de Manizales, para diseñar y administrar la plataforma tecnológica para el desarrollo de la educación a distancia asistida por medios virtuales e internet. Este sistema reduce la duración de los cursos de ascenso a 89 días presenciales para una mayor disponibilidad del personal en las Unidades aéreas.

Escuela de Suboficiales Fuerza Aérea Capitán Andrés M. Díaz, Esufa, Encargada de la Formación Tecnológica de la FAC

La Escuela de Suboficiales tiene la "misión de formar y capacitar integralmente al personal de Suboficiales de la Fuerza aérea; orientando sus políticas hacia la eficiencia de las técnicas de enseñanza, con miras a lograr un adecuado desarrollo tecnológico, acorde con la evolución de la aviación moderna". [28]

La creación de esta Escuela tiene sus orígenes desde el surgimiento mismo de la aviación militar y de la Escuela Militar de aviación, Ya mediante resolución 053 del 12 de agosto de 1971, se le denomino Escuela de Suboficiales Capitán Andrés M. Díaz. A partir de 1986, se exigió el título de bachiller a los aspirantes a ingresar a la Escuela de Suboficiales. Con este se cumplió uno de los requisitos para convertir a la Escuela en un Instituto de Formación Superior.

La Escuela obtuvo, según acuerdo ICFES 2754 del 5 de diciembre de 1991, la autorización para ofrecer y desarrollar programas de educación superior en la

---

[27] Ibid., p. 74
[28] Ibid., p. 75, 76.

modalidad tecnológica. A partir de octubre de 1992, el ICFES concedió la licencia de funcionamiento de las tecnologías en Administración Aeronáutica, Mantenimiento Aeronáutico, Tránsito Aéreo, Seguridad Aeronáutica, Electrónica Aeronáutica y actualmente Tecnología en Inteligencia Aérea. Ello llevo a aumentar de dos años y medio a tres anos la permanencia de los alumnos en la Escuela. En 1994, se inició el programa de Extensión para graduar los primeros Tecnólogos Aeronáuticos en Colombia. El 30 de noviembre de 1995, se efectuó la graduación de la primera promoción en cinco programas de pregrado: Mantenimiento Aeronáutico, Electrónica Aeronáutica, Comunicaciones Aeronáuticas, Administración Aeronáutica y seguridad y defensa de Bases. "En el mes de diciembre del 2011 se llevo a cabo la graduación de la primera promoción de Tecnología en Inteligencia Aérea";[29] lo cual abre un camino para la profesionalización.

3.2 CAPACITACION DEL PERSONAL DE LA FUERZA AÉREA EN CONOCIMIENTOS QUE PERMITAN EL DOMINIO DEL CIBERESPACIO, PARA LA CONDUCCIÓN DE OPERACIONES.

Uno de los puntos más importantes, y menos cuidados de las operaciones en el ciberespacio, son las competencias y habilidades de los ciberguerreros, y como esa actitud es capaz de inclinar la balanza hacia la victoria o la derrota.

Es necesario e imprescindible conocer a las tropas, saber hasta qué punto límite son capaces de llegar al implementar, desarrollar y conducir operaciones a través del ciberespacio, cuál es su compromiso con el propio bando.

---

[29] Ibid., p. 76.

La FAC siempre se ha preocupado por formar integralmente a su personal, por ello es de vital importancia abrir las puertas de la formación en el campo del ciberespacio, para implementar, desarrollar y conducir operaciones. Aunque es evidente que existe una formación pero todos son cursos o capacitaciones dictados por otras instituciones.(ver anexo C),que muchas veces no cumplen con la expectativas, porque no son enfocadas adecuadamente, para el cumplimiento de la misión.

Los cursos dictados a través de la figura de subcontratar son, extraido de las encuestas y confirmado por jefatura de desarrollo humano.

- ✓ Curso virtual de guerra electrónica.
- ✓ Curso ethical hacking (ECH)
- ✓ Especialista en seguridad de la información.
- ✓ Redes.
- ✓ Sistemas operativos.
- ✓ CCNA

Es necesario tener claridad, sobre cuáles son las instituciones que están dedicadas a impartir un conocimiento para el dominio del ciberespacio, a la FAC, ya que este análisis permite justificar la importancia de implementar una adecuada formación para el dominio del ciberespacio en la conducción, implementación y desarrollo de operaciones, desde una perspectiva militar, llenando así las expectativas del personal, este listado empresarial fue confirmado por desarrollo humano de la FAC.

- ✓ Empresa de administración bases de datos.
- ✓ Fontinet.
- ✓ Soft segurity
- ✓ Sena

- ✓ Universidad de los Andes.

Las capacitaciones deben ser enfocadas en formar ciberguerreros cualificados para la defensa, que tengan la capacidad de implementar, desarrollar y conducir operaciones en el ciberespacio. Por ello es importante conocer un poco de los perfiles de los ciberguerreros y sus comandantes, para evitar formar al personal de oficiales, suboficiales y civiles de la FAC, con un perfil no acorde con las necesidades de la fuerza, lo cual justifica la importancia de un adecuado eje temático, que incluya conocimientos sicológicos, al implementar una formación, para la implementación, desarrollo y conducción de operaciones en el ciberespacio.

- ➢ *"Ciberguerreros*

  Un ciberguerro, aunque cuente con más conocimientos o menos, con más experiencia o menos, solamente determina qué tipo de cometidos está capacitado para realizar, no si está preparado para realizarlo.

  Entrenar a un ciberguerrero es muy complicado, la personalidad de los expertos en seguridad informática suele estar teñida de tintes anarca, con tendencia a la individualidad, por lo que hacer que colaboren en grupo en pro de un único objetivo es una tarea ardua.

  Durante el año 2010 en el caso de Wikileaks, miles y miles de documentos confidenciales del ejército y cables oficiales. Posiblemente los controles internos de seguridad se hayan incrementado en ese país como consecuencia de las filtraciones"30.

- ➢ *Comandante*

---

[30] MONTERO, David. El arte de la guerra, Intelligence segurity. USA.2011.p.8,9

"Un comandante debe conocer la actitud de sus tropas, el entorno en el que se mueve, es capaz de dirigir la energía de las tropas hábilmente en batalla.

Un comandante debe tener conocimiento extenso acerca de la ciberguerra u operaciones de ataque-defensa en el ciberespacio, no de la guerra tradicional. La ciberguerra no trata de matar físicamente a una persona, no trata de tomar una posición en un monte, no trata de conquistar un cuartel, sino de entrar en una red, infectar con virus de guerra toda la red del enemigo para obtener información sensible de interés.

La ciberguerra no se ve, el sentido de la vista solamente confunde, en milésimas de segundo una batalla pasa de estar ganada a estar perdida.

Aunque perder una batalla no significa perder la guerra, sí condiciona la moral de los ciberguerreros y el devenir de futuras batallas.

Un comandante debe tener un sistema de comunicación rápido y estable con sus tropas, de manera que pueda modificar rápidamente la estructura de sus ciberguerreros, sus objetivos, sus tácticas, los equipos. El sistema de comunicación deberá ser resistente a contraataques, puesto que el enemigo también piensa, y sabe que destruyendo los sistemas atacantes o el sistema de comunicaciones detiene o dificulta en gran medida el ataque, puesto que los ciberguerreros actuarán de forma desorganizada o extremadamente ralentizada".31

3.3 LA CAPACIDAD DE LAS OPERACIONES EN EL CIBERESPACIO, COMO UNA ESTRATEGIA MILITAR.

Potencializar las capacidades de una fuerza, como la FAC, con personal altamente cualificado en temas de seguridad informática, manejo de redes, utilización y optimización del espacio electromágnetico; trae consigo el desarrollo de nuevas estrategias militares, La Estrategia Militar se define, según Lindell

[31] MONTERO, David. El arte de la guerra, Intelligence segurity. USA.2011.p.10

Hart[32], como el arte de distribuir y hacer actuar los medios militares para alcanzar los objetivos políticos, para contrarrestar el ataque del enemigo a través del ciberespacio y mecanismos de defensa en pro de mantener el control del espacio aéreo-espacial y contribuyendo así a la Seguridad Nacional. Todo esto hace necesario la implementación en sí de operaciones en el ciberespacio. Para ello es prudente tomar como referencia lo que ha pasado a lo largo de la historia a nivel mundial.

3.3.1 Infraestructura crítica.

Las instalaciones, redes, sistemas y equipos físicos y de tecnología de la información, cuyo funcionamiento es indispensable y no permite soluciones alternativas, por lo que su interrupción o destrucción tendría un grave impacto sobre los servicios públicos[33].

el mundo virtual y físico a través del ciberespacio, según Gibson, logran converger de una forma tal que las acciones desarrolladas en cada uno de estos, tiene repercusiones semejantes en el otro.[34]

Esta unión se ve reflejada que al generar un ataque, un actor determinado puede crear información maliciosa (virus, *malware*, etc) que está destinada a viajar por el ciberespacio hasta alojarse en el sistema informático deseado y ejecutar la acción para la que fue diseñada.

---

[32]MINISTERIO DE DEFENSA NACIONAL, Comando General Fuerzas Militares. Inteligencia Estratégica. Op Cit., p. 14.
[33] MINISTERIO DE DEFENSA. Ciberseguridad. Op Cit., p. 348
[34] GIBSON, William. Neuromancer. Acebooks, NY, 1984. p. 80

Si bien es entonces el objetivo la infraestructura crítica estatal, el concepto de Gibson se traduce al proyectar escenarios en donde: reactores nucleares pueden ser saboteados para que funcionen erróneamente; que hidroeléctricas abran sus compuertas sin control produciendo inundaciones a su paso; que un controlador aéreo deje de ver en su monitor el mapa real de vuelo de los aviones a su cargo; que los sistemas bancarios queden inservibles y las personas queden sin la posibilidad de acceder a sus recursos y apagar redes eléctricas dejando a poblaciones sin el funcionamiento que esta fuente de energía sustenta, serían algunas de las formas de comprender este vínculo *interdimensional*.[35].

3.3.1.1 Ataques cibernéticos

Es relevante dar a conocer los diferentes ataques cibernéticos a los cuales se han visto expuestos otros países de importancia mundial, para tomar como ejemplo y así planear una defensa en pro de la Seguridad Nacional.

> *Las primeras actividades conocidas relacionadas con la ciberguerra fueron los ataques coordinados desarrollados en 1999 sobre Estados Unidos por hackers desde un ordenador de Moscú (Rusia). Estos ataques fueron bautizados por el gobierno de EE.UU. como Moonlight Maze.*
>
> *Durante gran parte del año 2003, hackers de origen chino también atacaron de forma organizada a los Estados Unidos. Estos ataques fueron conocidos con el nombre clave Titan Rain.*
>
> *Durante Septiembre de 2007 países como Estados Unidos, Gran Bretaña, Francia y Alemania dieron a entender que China y su Ejército de Liberación Popular (EPL) estaban detrás de los ataques sufridos durante los últimos meses en sitios gubernamentales..*

---

[35] GAITAN RODRGUEZ, Andrés. Las guerras y sus generaciones. ESDEGUE, junio,2010. p.11.

El 14 de Diciembre de 2007 hackers de Estonia atacaron los proveedores de servicios de Internet de Kirguizistán mediante ataques de denegación de servicio y suplantaron la página oficial de la comisión electoral de dicho país.

Durante el año 2010 se produjeron ataques a equipos corporativos de Google desde direcciones IP residentes en Taiwan, después de una tensa situación debida a las restricciones que quería imponer China a su buscador. Después de los ataques se acusó al Gobierno de China de estar detrás de esta situación, y fue un tema que tuvo una importante repercusión en los medios de comunicación.[36]

Todos estos hechos nos muestran una aceleración en los actos de guerra a través del ciberespacio, lo que precisa de la implementación, desarrollo y conducción de operaciones en él.

No hay buenos datos existentes que precisen cuántas intrusiones cibernéticas se producen anualmente. El número es tan grande que en 2004, el gobierno de los EE.UU. dejó de informar el número de intrusiones conocidas, que en 2003 superó los 100.000 ataques cibernéticos. La mayoría de los expertos suponen que el número de hoy es un orden de magnitud mayor[37].

Así que el problema es grande. También es bastante complejo y nada sencillo debido a que, con la arquitectura actual de Internet, que es casi imposible de identificar la fuente de una intrusión," La red GhostNet ciber espionaje, evaluada recientemente por un canadiense del grupo de seguridad de información, con éxito perpetraron un sofisticado sistema de muchos ordenadores utilizados por los gobiernos y las organizaciones no gubernamentales que tenían contactos diplomáticos con China"[38]. Embajadas indias estaban infectadas, así como los

---

[36] MONTERO, David. El arte de la guerra, Intelligence segurity. Op Cit., p.5
[37] BUCCI, Steven. Cybersegurity, Heritage Foundation. Washington D.C. 2012.
[38] BUCCI, Steven. The National Security Risk, Heritage Foundation. Washington D.C. 2013.

sistemas del Dalai Lama de información. A través de sofisticados sistemas contra el hacking, el grupo canadiense fue capaz de rastrear la señal cibernética generada de los sistemas de control en Hainan, China (tal vez por casualidad, el hogar de una instalación de señales de inteligencia chino). Pero no podía ir más lejos. Así que, en realidad, nadie realmente sabe de dónde procedía "the GhostNet"; una realidad intrínseca de la naturaleza de la Internet.

3.3.1.2 Amenazas actuales.

Con un proceso de paz en marcha, es de resaltar la importancia de defender los sistemas informáticos, ya que pueden ser otra alternativa para que los grupos terroristas o guerrillas, vulneren la seguridad Nacional.

Para ello es necesario tener un dominio del ciberespacio y esto se logra a través de una formación adecuada y bien direccionada, para satisfacer las necesidades de la fuerza en pro de la Seguridad Nacional.

Actualmente, con el gran desarrollo de la tecnología y la necesidad de un mundo globalizado, crecen las amenazas en este campo; donde no hay una confrontación "cuerpo a cuerpo", sino que el enemigo puede llegar a ser muy silencioso; pero logra desestabilizar económica y socialmente a la nación. No todas las amenazas a la seguridad nacional nacen de la criminalidad cibernética. En los supuestos mencionados –terrorismo y criminalidad organizada–se considera que determinadas formas de cibercriminalidad representan verdaderas amenazas a la seguridad nacional.[39]

3.3.2 Capacidades de otros países

---

[39] MINISTERIO DE DEFENSA. Ciberseguridad. Op Cit., p.326

Dados los innumerables ataques cibernéticos a los cuales se han visto expuestos, los diferentes países, estos han tomado algunas medidas que sirven de ejemplo a Colombia. Es el caso de España, que en el 2009 creo el Centro Nacional para la Protección de las Infraestructuras Críticas; que tiene como finalidad salvaguardar las redes eléctricas, telecomunicaciones, sistema financiero, entre otros.

Es interesante mencionar a Cyber Storm, los ejercicios desarrollados por Estados Unidos durante 2006 y 2008, que con la cobertura de ser juegos de guerra, eran escenarios de defensa ante posibles ataques informáticos a gran escala, donde estaban implicados numerosos expertos en seguridad informática de diversas agencias gubernamentales y entidades financieras. El primer ejercicio tenía como atacante delincuentes informáticos contratados por un grupo terrorista. El segundo ejercicio, durante marzo de 2008, tenía como atacante un país sin determinar. El ejercicio que se celebró durante el año 2010 tuvo como invitados a doce países occidentales de los cuales siete eran europeos.

> *"Potencias emergentes como China, se han preparado a conciencia también en la ciberguerra durante los últimos años, consistente en la formación altamente especializada de ciberguerreros, en simulacros de intrusiones en redes enemigas, además de defensa contra ataques exteriores.*
>
> *También durante el 2010 se realizó una simulación de ciberataque en Estados Unidos, bajo la premisa de la inutilización de las redes eléctricas del país.*
>
> *Todo esto se agravó por el hecho de que Estados Unidos fue la primera potencia mundial en crear un cuarto ejército para la protección de su nación, comandos de ciberguerreros entrenados y preparados para el combate en el ciberespacio, y a su vez, nombrara un mando militar como responsable de ese cuarto ejército: un ciberzar, el general John Andrews".*[40]

---

[40] Ibid., p.6

Estado Unidos es un ejemplo que ha avanzado en la conducción de operaciones en el ciberespacio y han planteado tres pilares en su esfuerzo por hacer de Estados Unidos un competidor sólido en este campo.

> *Aliados fuertes. El ciberespacio no es un salvaje oeste ingobernable. Las naciones pueden actuar dentro de su soberano ciberespacio, donde la infraestructura está dentro de sus fronteras. Los EE.UU. deben trabajar en conjunto con los países de ideas afines comprometidos con la libertad, la prosperidad y la seguridad para luchar contra los malos actores en el ciberespacio. La Ciberseguridad se está convirtiendo en una cuestión cada vez más importante para la OTAN. Los EE.UU. deberían estar construyendo fuertes alianzas con naciones como la India también.*
>
> *Fuertes líderes cibernéticos. La edad en que las cuestiones cibernéticas fueron el director de información del problema-ya sea en el gobierno o el sector privado se ha acabado. Los líderes de gobierno y el sector privado deben desarrollar las habilidades, conocimientos y atributos de liderazgo en ciberseguridad. Ellos necesitan la educación, la formación y la experiencia que califica para ser líderes reales cibernéticos.*
>
> *Fuertes ciudadanos cibernéticos. La actividad en línea más malicioso ocurre con tan poco esfuerzo debido a las malas prácticas de seguridad individuales. Muchos caen víctima a los más torpes de "ingeniería social" artimañas utilizadas para robar contraseñas o inyectar virus en las redes informáticas, como hacer clic en un enlace que dice: "Tienes que ver esto."*[41]

3.3.3 Capacidad de Colombia para enfrentar la amenaza CONPES 3701.

El CONPES o Consejo Nacional de Política Económica y Social.

---

[41] BUCCI, Steven. Individual ciber-preparación es la defensa civil del siglo 21. The heritage fundation. Washington D.C. 2012. p.33

Dentro de este documento se traza como objetivo central de esta política el fortalecimiento de la capacidad del Estado para enfrentar las amenazas que atentan contra su seguridad y defensa en el ámbito cibernético, y a su vez se definen tres objetivos específicos:

1) Implementar instancias apropiadas para prevenir, atender, controlar y generar recomendaciones que regulen los incidentes y/o emergencias cibernéticas para proteger la infraestructura crítica nacional;

2) Diseñar y ejecutar planes de capacitación especializada en ciberseguridad y ciberdefensa; y

3) Fortalecer el cuerpo normativo y de cumplimiento en la materia.

Las Fuerzas militares día tras día deben reevaluar la estrategia militar y modernizar la capacidad de inteligencia y combate" [42]. Lo que provoca, que La Fuerza Aérea acelere la adopción de nuevas tecnologías y una visión más amplia de sus comandantes, en cuanto, a la importancia que se merece, la implementación, desarrollo y conducción de operaciones a través del ciberespacio; la simbiosis del talento humano, producto de la formación integral y la tecnología como fuerza dominante y decisiva que los conducirá a la victoria. Lo que implica ventajas decisivas: reduce los riesgos para los integrantes de la institución, optimiza los recursos económicos y potencializa los recursos humanos, mejora la habilidad para identificar y atacar todo tipo de blanco aun en condiciones adversas, logra mayor precisión en los ataques para reducir las víctimas y la destrucción, minimiza los efectos colaterales de la guerra y alcanza resultados exitosos dentro de un marco de respeto a los Derechos Humanos, DD.HH., al

---

[42] FUERZA AÉREA COLOMBIANA. Vocación de victoria. Op Cit., p. 141.

Derecho Internacional humanitario, DIH, y al Derecho Internacional de los Conflictos Armados, DICA.

Los responsables políticos deben tratar con el mundo tal como es, no como se desearía que fuese. Toda legislación debe lidiar con el Internet como lo es hoy, no como los EE.UU. espera que sea en el futuro.

En Colombia el Ministerio de Defensa lidera los temas de "ciberseguridad y ciberdefensa, a través de colCERT (equipo de respuesta a emergencias informáticas de Colombia), coordina las acciones necesarias para la protección de la infraestructura crítica del estado colombiano"[43].

3.3.4 Evolución de las guerras

El surgimiento de los Estados nacionales en la era moderna trajo el desarrollo de la guerra de primera generación (1 GW), también conocida como la guerra napoleónica, con su utilización de los ejércitos contra otros en línea masiva y formaciones de columnas. Como resultado de la revolución industrial y las mejoras cuantitativas y cualitativas en la potencia de fuego se llega a las guerras de Segunda Generación (trinchera) (2GW), la cual hizo su aparición durante la Guerra Civil Americana, y poco a poco ha reemplazado la guerra de Primera generación (1 GW). Esto culminó con la guerra de trincheras y matanzas en masa de los ejércitos que se produjeron en Europa durante la Primera Guerra Mundial. Guerra de Tercera Generación (maniobra) (3 GW) fue concebida por los alemanes durante la Primera Guerra Mundial, y más tarde presentó al comienzo de la Segunda Guerra Mundial por la Wehrmacht alemana con su conquista de Europa. Fue el resultado de mejoras en la tecnología disponible y se caracteriza por las

---

[43] MINISTERIO DE DEFENSA, Dirección de estudios sectoriales. Dirección de programas, Bogotá. 2009.p.5.

operaciones de armas combinadas; mar, aire y tierra, caracterizada por la rápida maniobra de las formaciones mecanizadas. La guerra de Tercera Generación (maniobra) (3 GW) ha sido la forma dominante de la guerra convencional militar entre los Estados-nación, incluyendo los Estados Unidos, en la época moderna.

La guerra de Cuarta Generación (insurgentes) (4GW) es un concepto originado por William S. Lind, y reafirmado por Hammes. Su aplicación fue concebida por Mao Tse Tung durante la revolución china de 1925-1927, y se utiliza con éxito para derrotar a los ejércitos nacionalistas de Chang Kai-shek al instalar un gobierno comunista en China. Cuarta Generación (insurgentes) (4GW) tiene varias características que le dan una ventaja sobre la guerra de Tercera Generación (maniobra) (3 GW) la cual permitió cuantitativa y cualitativamente a las fuerzas inferiores imponerse sobre las fuerzas gubernamentales superiores. Se utiliza la estrategia y las tácticas asimétricas, aplicadas durante largos períodos de tiempo. Conduciendo la derrota del enemigo a través de su voluntad política . Coincide con la fuerza política de un adversario en contra de la fuerza política de la otra. En su forma más común es la guerra de insurgencia. Fue adaptado y utilizado con éxito por los norvietnamitas para derrotar a los Estados Unidos, por los afganos para derrotar a la Unión Soviética, y está siendo utilizado por Al Qaeda hoy en su insurgencia global.

La guerra de Cuarta Generación (insurgentes) (4GW) se caracteriza por el uso de las redes, que está dispuesto a aceptar bajas, y su larga duración en el tiempo. Se mide en décadas más que en campañas que duran meses o años. Los chinos comunistas lucharon durante veintisiete años, los vietnamitas lucharon contra los franceses, y más tarde los norteamericanos, durante treinta años;. Y los afganos, con el apoyo de otras naciones, lucharon contra los soviéticos durante diez años.

Cuarta Generación (insurgentes) Guerra (4GW) se sitúa único hasta el momento como el único tipo de guerra que ha derrotado a una superpotencia, y así lo ha hecho en dos ocasiones.

Ciberguerra 5GW

La Guerra de Quinta generación (5 GW) se define como el uso de "*todos los medios que sea - medios que involucran la fuerza de las armas y los medios que no impliquen la fuerza de las armas, los medios que implican el poder militar y los medios que no impliquen el poder militar, significa que conllevan bajas, y los medios que no impliquen bajas para obligar al enemigo a servir al interés propio*"[44].Incluye la aparición de individuos súper-empoderados y grupos con acceso a conocimiento moderno, la tecnología y los medios para llevar a cabo ataques asimétricos en cumplimiento de sus derechos individuales y los intereses de grupo. Podría decirse que sus manifestaciones identificables primero ocurrieron en Estados Unidos durante los ataques con ántrax de 2001 y los ataques de la ricina de 2004. Ambos conjuntos de ataques requieren conocimientos especializados, incluidos los ataques contra oficinas del gobierno federal y las instalaciones, lograron interrumpir los procesos gubernamentales, y ha creado un temor generalizado en el público. "Hasta la fecha, ningún individuo o grupo se ha atribuido la responsabilidad de ninguno de los ataques, y tampoco que el ataque haya sido resuelto. Los ataques tuvieron bastante éxito en la interrupción de los procesos de gobierno y crear temor público, pero, hasta el momento, su motivación sigue siendo desconocido"[45].

Los piratas informáticos de hoy en día, capaces de perturbar los gobiernos y corporaciones a nivel mundial por atacar a la Internet, con programas informáticos maliciosos, también pueden ser precursores de individuos súper-empoderados y

---

[44] NEWSLETTER, IA. Army, Navy, Air forcé, and cyber-is it time for a cyberwarfare Branch of military. Washington D.C.2009. Vol 12. No 1. p.1

[45] NEWSLETTER, IA. Army, Navy, Air forcé, and cyber-is it time for a cyberwarfare Branch of military. Washington D.C.2009. Vol 12. No 2. p.12

grupos. Ellos ya han demostrado que son capaces de emprender en solitario campañas tecnológicas con visos de quinta generación Guerra (5 GW).

El poder potencial de quinta generación (5 GW) se demostró también en los atentados de Madrid de 2004. En esta ocasión, una serie de atentados de transporte público a cargo de un grupo terrorista en red en un solo día, en vísperas de las elecciones nacionales, dio lugar a un nuevo gobierno español de ser votado en la oficina, y la inmediata retirada del apoyo militar español a la coalición en curso operaciones contra la insurgencia en Irak. Los atentados de Madrid son significativos porque los terroristas detrás de ellos fueron también los principales distribuidores de drogas, parte de una red que va desde Marruecos a través de España a Bélgica y los Países Bajos. A pesar de los atentados de Madrid se cree que han costado sólo unos 50.000 dólares para llevar a cabo, las autoridades policiales luego recuperaron casi $ 2 millones en drogas y dinero en efectivo.

En estos ataques, un grupo representó una extensa empresa transnacional criminal con éxito a un cambio de régimen en una nación soberana europea. Al hacerlo, demostró cómo la Guerra de quinta generación (5 GW) tiene una ventaja dialéctica cualitativa sobre los métodos tanto de Tercera Generación (maniobra) Guerra (3 GW) y Cuarta Generación (insurrección) Warfare (4GW)[46].

3.3.5 Ambientes de empleo del poder aéreo y espacial

El desarrollo vertiginoso de la tecnología ha transformado el mundo y ha generado nuevos ambientes de combate o ambientes operacionales. Tradicionalmente, la guerra se adelantaba en tierra, agua y aire; hoy en día, y gracias a la evolución tecnológica, han surgido dos nuevos ambientes de combate: el espacio (región del

---

[46] QUINTERQ, Sirio. El arquitecto y la guerra de quinta generación, El sudamericano. México. D.C. 2011.p.70.

universo que se encuentra más allá de la atmósfera terrestre) y el ciberespacio (ámbito artificial creado por el hombre, caracterizado por el uso de componentes electrónicos y el espectro electromagnético para guardar, modificar e intercambiar datos a través de sistemas de redes e infraestructuras físicas). Estos ambientes de combate se convierten a la vez en ambientes de empleo, en los que, de acuerdo a sus características y capacidades, el Poder Aéreo y Espacial debe interactuar[47].

3.3.6 Características del ciberespacio

Para implementar, desarrollar y conducir una operación en el ciberespacio, se debe tener muy claro, que se esta defendiendo o atacando la información a través de la red, haciendo uso del espectro electromagnético; lo que nos lleva a precisar los conocimientos del ciberataque y ciberdefensa. Las disposiciones hacen referencia a la preparación que deben tener los ciberguerreros de cara al combate: cuándo atacar y cuándo defender. Conocer estos principios es fundamental para que un ataque o una defensa sean exitosos.

---

[47] FUERZA AÉREA COLOMBIANA. MANUAL DE DOCTRINA BÁSICA AÉREA Y ESPACIAL, Bogotá. Cuarta Edición. 2013.p.23

Mandar sobre muchos ciberguerreros es lo mismo que mandar sobre pocos, es una cuestión de organización. Al igual que dirigir un gran ejército es lo mismo que dirigir a unos pocos ciberguerreros, es una cuestión de comunicación.

La organización y la comunicación determinan la eficiencia del ataque y la defensa, puesto que la suma del todo es menor que la suma de las partes individuales. Cuanta mayor organización y mejor sea el sistema de comunicaciones, más se aproximara hacia la igualdad.

"De esta manera, un ejército moderno de ciberguerreros debería estar compuesto por funcionalidades de la siguiente manera"[48]:

ATAQUE

↓

Expertos en perimetrales

↓

Expertos en intrusión

↓

Expertos en virología

DEFENSA

↓

Expertos en perimetrales

↓

Expertos en virología

↓

Expertos en contingencia

↓

Expertos en defensa contra intrusión

[48] MONTERO, David. El arte de la guerra, Intelligence segurity. Op Cit., p.11

Cualquier acción que interrumpa el flujo de la información puede afectar a la organización. Para evitar esto, hay tres grandes rubros de ciberdefensa que debemos mantener, conocido como CID.

> *"Confidencialidad: consiste en darle acceso a la información solo a la persona correcta, en el momento y lugar correcto.*
>
> *Integridad: consiste en evitar que la información sea modificada por gente o máquinas no autorizadas.*
>
> *Disponibilidad: consiste en asegurar que la información este disponible para ser utilizada por las personas o máquinas autorizadas cuando lo requieran".*[49]

En el ámbito del ciberataque, podemos decir que el objetivo del hacker es lograr violentar el CID dela organización objetivo con las siguientes acciones, conocidas como EMD.

> *"Extracción: consiste en penetrar los sistemas de la organización y obtener información considerada como confidencial.*
>
> *Modificación: consiste en cambiar la información almacenada en los sistemas del contrincante para causar algún tipo de disrupción en sus procesos.*
>
> *Denegación de servicio: consiste en saturar o apagar los sistemas del contrincante para que no pueda tener acceso a su información"*[50].

Estos procesos de ciberdefensa y ciberataque, junto con los cuatro factores fundamentales a la hora de valorar la guerra, se hace necesario compararlos en el caso de contienda de cara a determinar el resultado. Los factores son: política, terreno, comandante y doctrina.

---

[49] CASTRO Reynoso, Sergio. Arquitectura de seguridad informática, Charleston sc. USA. 2013.p.13,14

[50] Ibid., p.14

"La política hace referencia a la armonía de los ciberguerreros con sus dirigentes, hasta dónde son capaces de llegar por su comandante en la batalla.

El terreno implica el ciberespacio, la red donde se celebra el combate, la conectividad existente entre las distintas subredes.

El comandante se refiere al oficial que comanda los ciberguerreros, siendo necesario la existencia de unas determinadas cualidades: sabiduría, sinceridad, coraje y disciplina.

La doctrina se entiende como la organización de los ciberguerreros, las distintas graduaciones y rangos que puedan existir, además de la regulación de las conexiones existentes con la red enemiga."[51]

Los cuatro factores han de ser conocidos por cada comandante. Aquel que llega a dominarlos, vence; aquel que no, sale derrotado.

Para implementar, desarrollar o conducir una operación en el ciberespacio ya sea de ataque o defensa se debe tener en cuenta los siguientes criterios, que ayudaran a optimizar y a disminuir el margen de error en las operaciones.

"El Arte de la Ciberguerra se basa en el engaño. Cuando se ataca hay que aparentar cierta incapacidad, dejar que los defensores se confíen, hasta que es demasiado tarde. Aparentar estar lejos del objetivo cuando realmente se está cerca proporciona una ventaja fundamental.

Muestra una o dos conexiones activas a la red enemiga y oculta el resto de ciberguerreros que están invadiendo el terreno, de manera que los defensores piensen que el atacante cuenta con menos efectivos. Esto hará que se relajen y piensen que es una incursión ocasional, una exploración.

---

[51] MONTERO, David. El arte de la guerra, Intelligence segurity. Op Cit., p.15

Si notas que las tropas enemigas se encuentran bien organizadas, intenta desorganizarlas, no ataques directamente. Ataca al enemigo cuando no esté preparado, en rangos horarios de poca actividad.

Todas las estimaciones hay que valorarlas previo al inicio de una batalla. Si las estimaciones indican victoria, es porque los cálculos muestran que tus condiciones son más favorables que las de tu enemigo; si indican derrota, es porque muestran que las condiciones favorables para la batalla son menores.

En este caso, no ataques.

Con una evaluación cuidadosa, uno puede vencer; sin ella, no puede. El estudio previo es determinante, por lo que cualquier sistema de apoyo a la decisión, como un simulador de ciberguerra, puede ayudar a la evaluación."[52]

Para la preparación al implementar, desarrollar o conducir las operaciones a través del ciberespacio, es ideal contar con un simulador de ciberguerra, las características que se deberían encontrar en un buen simulador de ciberguerra son diversas, aunque todas deben confluir en un único punto: generar conocimiento y experiencia en los ciberguerreros. Éstas características son.

***"Entorno real**. Para generar un mundo real se aconseja el uso de máquinas virtuales capaces de modelar un sistema de gestión de red propio que simule el espacio IPv4/IPv6 y la red enemiga. La generación de simulaciones deberá realizarse nutriéndose de datos reales para poder crear un entorno de infraestructuras y aplicaciones virtuales.*

***Interacción con el enemigo**. El simulador deberá ser capaz de reaccionar ante las agresiones de forma similar a como podría hacerlo un defensor entrenado mediante reglas de acción definidas y basadas en inteligencia artificial: conocer quien está atacando y proteger los sistemas.*

---

[52] Ibid., p.16

***Aprendizaje**. El simulador debe ser capaz de otorgar aprendizaje a los ciberguerreros. No basta con aprender a realizar una intrusión con éxito en un determinado sistema, deben aprender a combatir en la ciberguerra, a esperar lo inesperado.*

Construir un simulador de este tipo es una tarea ardua pero no imposible, la aparición de potentes tecnologías de virtualización han facilitado enormemente la creación de este tipo de simuladores, solamente hacen falta los recursos."[53]

Para hacer las operaciones a través del ciberespacio se requiere de sigilo, organización y saber liderar y direccionar las capacidades de los ciberguerreros, clasificándolos teniendo en cuenta sus capacidades y experiencia, para así mantenerlos motivados; lo cual es clave para alcanzar la victoria.

"Las operaciones bélicas que componen la ciberguerra y las motivaciones de porqué es necesaria una victoria rápida, de manera que se impida un desgaste continuado de recursos y moral en los ciberguerreros.

La ciberguerra es una guerra de guerrillas, atacar y retirarse, y volver a empezar, un continuo combate intelectual, de astucia, sigilo y engaño. No tenemos que olvidar que en el fondo, es mucho más humano el combate entre ciberguerreros que el combate entre guerreros de la antigüedad, puesto que antes se combatía físicamente, y ahora intelectualmente.

La naturaleza innata de las comunicaciones a través de Internet posibilita acceder al terreno enemigo con un coste mínimo, no así mantener las conexiones establecidas. El principal objetivo de los ciberguerreros será obtener una victoria rápida sobre el enemigo. De no ser así, la moral de los ciberguerreros se resentirá de sobremanera, el consumo de recursos que supondrá mantener la campaña será elevado y la confianza de los patrocinadores disminuirá.

Los ciberguerreros verdaderamente hábiles son capaces de capturar recursos tecnológicos del enemigo sin batallar prácticamente, limitando el acceso y las

---

[53] Ibid., p.14

comunicaciones exteriores una vez que han accedido a los mismos. El resultado se traduce en ataques limpios, que no desembocan en campañas alargadas, y con la captura de los recursos deseados, para posteriormente mantener o inutilizar los recursos, según haya establecido el comandante al mando."[54]

La victoria en la ciberguerra, al conducir operaciones en el ciberespacio, se puede predecir, puesto que se basa en cánones medibles. Obtener la victoria implica lograr los objetivos propuestos: inutilizar, apropiarse o alterar un recurso tecnológico, destruir las capacidades de los ciberguerreros enemigos.

Hay cinco casos en los que se puede predecir la victoria:

"El que sabe cuándo luchar y cuándo no, saldrá victorioso.

El que comprende cómo luchar, de acuerdo con las fuerzas del adversario, saldrá victorioso.

Aquél cuyas filas estén unidas en un propósito, saldrá victorioso. Este punto está relacionado con la motivación de los ciberguerreros.

El que está bien preparado y descansa a la espera de un enemigo que no esté bien preparado, saldrá victorioso. El factor sorpresa es fundamental en la ciberguerra, donde el tiempo transcurre más rápido que en otros entornos.

Aquel cuyos comandantes son capaces y no sufren interferencias de sus dirigentes, saldrá victorioso. Un comandante con cualidades que sea capaz de dirigir a los ciberguerreros, y no reciba continuamente órdenes contradictorias de sus dirigentes, tendrá mayores posibilidades de victoria."[55]

---

[54] Ibid.,p.19
[55] Ibid.,p.20

En definitiva, podemos concluir que la victoria puede ser obtenida sin empezar si quiera las operaciones en el ciberespacio en caso de que el enemigo no esté preparado.

Ya que la ciberdefensa se lleva a cabo a través del ciberespacio es importante entender en que consiste exactamente; es por eso que se identificaran todos los elementos del ciberespacio, que nos permiten transmitir y recibir información de todo tipo y sus características.

> *"Servidores: son computadoras de alto desempeño, que tienen la función de servir información.*
>
> *PCs: Son computadoras personales, que permiten administrar nuestra información y conectarnos a servidores en internet.*
>
> *Smartphone y tabletas: Estos teléfonos son una pequeña computadora.*
>
> *Elementos de red: son los switches, ruteadores, firewalls y servidores de DNS, los cuales administran el flujo de datos a través de la red.*
>
> *Sistemas SCADA: Scada significa control de supervisión y adquisición de datos, este tipo de aparatos controlan todo tipó de procesos industriales.*
>
> *Otros aparatos: cada vez hay más aparatos que pueden conectarse a la red, tales como los teléfonos de voz sobre IP, sistema de audio y videoconferencia, cámaras e impresoras de red. También comienzan a aparecer automóviles con conexión de red, y conforme avance la tecnología, veremos cada vez más y más aparatos de todo tipo con conectividad a la red."*[56]

No hay valoraciones de fondo de la seguridad en el ciberespacio que es de una cierta longitud legible y que podría dar inicio al estudio y sondeo con profundidad

---

[56] CASTRO Reynoso, Sergio. Arquitectura de seguridad informática, Charleston sc. Op Cit., p.3,4.

respecto a la materia. Sin embargo, es importante comenzar en alguna parte. Este examen comienza con lo que se sabe sobre la naturaleza actual de la Internet y el ciberespacio. A continuación se presentan 10 verdades sobre el ciberespacio:

1. Los ataques cibernéticos son indirectos
2. El ciberespacio está en todas partes
3. La Internet no tiene fronteras
4. El anonimato es una característica, no un error
5. Líneas Maginot Nunca trabaje en el largo plazo
6. Entre el 85% y 90% del tráfico Gobierno de EE.UU. viaja a través de redes no gubernamentales.
7. Hay un papel legítimo para el gobierno.
8. La NSA (Agencia Nacional de Seguridad) lo hace mejor que DHS (Departamento de Seguridad Nacional).
9. Ninguna defensa será siempre 100 % perfecta.
10. Los ataques de hardware son aún más difíciles de prevenir que los ataques de software.

3.3.7 Empleo de las Aeronaves no Tripuladas en el Desarrollo de Operaciones.

Los ART o Aeronaves no tripuladas, han tenido un gran desarrollo y en la actualidad realizan misiones de reconocimiento aéreo de nivel táctico, operacional y estratégico, es por ello que son vulnerables al ciberataque, ya que son operados a través del ciberespacio.[57]

---

[57] FUERZA AÉREA COLOMBIANA. Manual de Inteligencia Aérea, Fuerzas Militares. Bogotá, 2010l p. 36,37.

Las aeronaves no tripuladas, son aeronaves que son operadas desde estaciones terrestres o trasportadas por otra aeronave, desde una zona de seguridad con el fin de operar en zonas de presencia enemiga, con el fin de minimizar los costos tanto económicos como humanos ante eventuales accidentes o derribos. Estas aeronaves pueden cumplir múltiples misiones de acuerdo a los equipamientos tecnológicos con los cuales se les haya dotado, siendo la principal limitante el espacio y el peso de los mismos, la principal bondad de estas aeronaves es su autonomía la cual en casi todos los equipos debido a su bajo consumo de combustible esta entre 14 y 20 horas, tiempo suficiente para que se efectúen excelentes reconocimientos aéreos.

El radio de operación de los equipos varía de acuerdo al equipo y al sitio en el cual se encuentre ubicada la antena trasmisora de comunicaciones, tienen la ventaja de transmitir en tiempo real las imágenes de lo observado a los centros de control para la toma de decisiones por parte de los comandantes.

De acuerdo al equipo pueden contar, en algunos casos, con telémetros muy precisos para una adecuada ubicación y georeferenciación de los objetivos y sus elementos adyacentes, siendo fundamentales para la toma de decisiones, principalmente en lo referente a la salvaguarda de los bienes protegidos por el DICA y el DIH en las operaciones militares; adicionalmente dicha virtud puede en un momento dado permitir que estas aeronaves sirvan como controlador aéreo avanzado para el control de la entrega de armamento.

4 MARCO INSTITUCIONAL Y LEGAL

Una Fuerza aérea Desarrollada tecnológicamente, con el mejor talento humano y afianzada en sus principios y valores, para liderar el poder aéreo y espacial y ser decisiva en la defensa de la nación.

Desarrollada tecnológicamente: El desarrollo en todos los ambientes de la fuerza aérea, es la orientación hacia un futuro deseado no solo por la comunidad aérea, sino por el pueblo colombiano. Ese objetivo más que un sueño, es la realidad y cualidad que permanentemente desarrollara la Fuerza Aérea Colombiana, mediante la promoción e impulso del desarrollo científico y tecnológico que le permita un desarrollo de la industria aérea, espacial y de defensa y convertirse en una autoridad aeronáutica que confluya en la contribución y el desarrollo de la industria nacional.

Para liderar el poder aéreo y espacial: mediante el desarrollo tecnológico como puerta de acceso para avanzar en conocimiento sobre la tierra y el espacio ultraterrestre, mediante el uso de tecnologías modernas que permitan la conectividad, la comunicación con todo el territorio nacional, utilizando técnicas espaciales de telecomunicaciones, así como la implementación de tecnología de aplicación a la "aeronavegación y por otro lado el uso de información proveniente de sensores remotos para la observación de la tierra, de tal forma que incremente la productividad y efectividad de los distintos sectores, que demandan información

Geoespacial y reconozcan en la Fuerza Aérea como una organización poseedora de los conocimientos requeridos para liderar el poder aéreo y espacial"[58].

CONPES 3701: Consejo Nacional de Política Económica y Social.

Dentro de este documento se traza como objetivo central de esta política el fortalecimiento de la capacidad del Estado para enfrentar las amenazas que atentan contra su seguridad y defensa en el ámbito cibernético, y a su vez se definen tres objetivos específicos: 1) Implementar instancias apropiadas para prevenir, atender, controlar y generar recomendaciones que regulen los incidentes y/o emergencias cibernéticas para proteger la infraestructura crítica nacional; 2) Diseñar y ejecutar planes de capacitación especializada en ciberseguridad y ciberdefensa; y 3) Fortalecer el cuerpo normativo y de cumplimiento en la materia.

Misión de la FAC: La Fuerza Aérea Colombiana ejerce y mantiene el dominio del espacio aéreo y conduce operaciones aéreas, para la defensa de la soberanía, la independencia, la integridad territorial nacional, del orden constitucional y el logro de los fines del Estado.

La Doctrina Aérea y Espacial se refiere a las directrices que orientan el empleo de los recursos relacionados con el uso del espacio aéreo y a la explotación del espacio ultraterrestre para un fin determinado.

La existencia de la FAC se fundamenta legal y doctrinariamente en el artículo 217 de la Constitución Política de Colombia, que dice:

---

[58] FUERZA AÉREA COLOMBIANA. Plan estratégico institucional2011-2030, Bogotá. 2011.p.5.

"La Nación tendrá para su defensa unas Fuerzas Militares permanentes constituidas por el Ejército, la Armada y la Fuerza Aérea. Las Fuerzas Militares tendrán como finalidad primordial la defensa de la soberanía, la independencia, la integridad del territorio nacional y del orden constitucional"[59].

Como referentes de la normativa nacional en la materia, es importante hacer mención a los esfuerzos realizados por Colombia en su legislación de manera cronológica, tal como se observa a continuación.

Es importante y cabe destacar, el gran interés, esfuerzo, integración e innovación que se ha generado entorno al tema de ciberseguridad, tanto de los organismos inter-agenciales tanto del mismo estado en pro de fortalecer las medidas tendientes a la protección de los intereses nacionales. Es así como las FFMM y de Policía, han visto la necesidad de crear a nivel interno, grupos especializados en conservar la integridad de la información y de su infraestructura la cual está ligada a la seguridad y defensa nacional.

Ley 527 de 1999 - COMERCIO ELECTRÓNICO: Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones"

Ley 599 DE 2000: Por la cual se expide el Código Penal. En esta se mantuvo la estructura del tipo penal de "violación ilícita de comunicaciones", se creó el bien jurídico de los derechos de autor y se incorporaron algunas conductas relacionadas indirectamente con el delito informático, tales como el ofrecimiento, venta o compra de instrumento apto para interceptar la comunicación privada

---

[59] MINISTERIO DE DEFENSA, Fuerza aérea colombiana. Manual de doctrina aérea. Bogotá, 2011.p.3

entre personas. Se tipificó el "Acceso abusivo a un sistema informático", así: "Art. 195. El que abusivamente se introduzca en un sistema informático protegido con medida de seguridad o se mantenga contra la voluntad de quien tiene derecho a excluirlo, incurrirá en multa."

Ley 962 de 2005: Por la cual se dictan disposiciones sobre racionalización de trámites y procedimientos administrativos de los organismos y entidades del Estado y de los particulares que ejercen funciones públicas o prestan servicios públicos. Prevé el incentivo del uso de medios tecnológicos integrados para disminuir los tiempos y costos de realización de los trámites por parte de los administrados.

Ley 1150 de 2007: Por medio de la cual se introducen medidas para la eficiencia y la transparencia en la Ley 80 de 1993 y se dictan otras disposiciones generales sobre la contratación con Recursos Públicos. Específicamente, se establece la posibilidad de que la administración pública expida actos administrativos y documentos y haga notificaciones por medios electrónicos, para lo cual prevé el desarrollo del Sistema Electrónico para la Contratación Pública, Secop.

Ley 1273 de 2009: Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.

Ley 1341 de 2009: Por la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las tecnologías de la Información y las Comunicaciones –TIC, se crea la Agencia Nacional del Espectro y se dictan otras disposiciones.

Resolución de la Comisión de Regulación de Comunicaciones 2258 de 2009: Sobre seguridad de las redes de los proveedores de redes y servicios de

telecomunicaciones. Esta resolución modifica los artículos 22 y 23 de la Resolución CRT 1732 de 2007 y los artículos 1,8 y 2,4 de la Resolución CRT 1740 de 2007. Esta regulación establece la obligación para los proveedores de redes y/o servicios de telecomunicaciones que ofrezcan acceso a Internet de implementar modelos de seguridad, de acuerdo con las características y necesidades propias de su red, que contribuyan a mejorar la seguridad de sus redes de acceso, de acuerdo con los marcos de seguridad definidos por la UIT, cumpliendo los principios de confidencialidad de datos, integridad de datos y disponibilidad de los elementos de red, la información, los servicios y las aplicaciones, así como medidas para autenticación, acceso y no repudio. Así mismo, establece obligaciones a cumplir por parte de los proveedores de redes y servicios de telecomunicaciones relacionadas con la inviolabilidad de las comunicaciones y la seguridad de la información.

Circular 052 de 2007 (Superintendencia Financiera de Colombia): Fija los requerimientos mínimos de seguridad y calidad en el manejo de información a través de medios y canales de distribución de productos y servicios para clientes y usuarios.

"*La visión establece que la Fuerza Aérea del futuro sea una organización militar con participación decisiva en la defensa de la nación, con hombres y mujeres que aporten lo mejor de su talento y experiencia, para el cumplimiento de la misión asignada*".60

Por lo anterior, este proyecto requiere el apoyo y revisión permanente de la Jefatura de Educación Aeronáutica, la Jefatura de Operaciones Aérea y la Jefatura de Inteligencia Aérea, como entes rectores y encargados de la formación integral

---

[60] FUERZA AÉREA COLOMBIANA. Vocación de victoria. Op. Cit., p. 52

del personal de la FAC y el manejo de los recursos para optimizar las operaciones en pro de la Seguridad Nacional.

5 MATERIAL Y MÉTODOS

5.1 ENFOQUE DEL PROYECTO

El estudio que justifica la importancia y necesidad de formar personal calificado en la FAC, para implementar, desarrollar y conducir operaciones en el ciberespacio, como una estrategia militar, es un proyecto que tiene características de investigación y acción, donde se aplica y amplia un conocimiento tomando como base otra estructura ya establecida, para lograr prestar un mejor servicio integral en pro del desarrollo de la fuerza.

Es un proyecto de tipo aplicativo cuya metodología se basa en elementos cuantitativos, ya que se trabaja sobre instrumentos medibles, como encuestas y teniendo como base los resultados se procede a realizar las entrevistas, que nos permiten presentar un estudio objetivo que justifica la necesidad de formar personal calificado en la FAC, para la implementación, desarrollo y conducción de operaciones en el ciberespacio, como una estrategia militar.

El proyecto se plantea desde tres perspectivas: en primera instancia, se analiza la información recolectada dentro de la FAC respecto al tema en mención y en segunda instancia se procede a diseñar las encuestas para ser aplicadas y de allí extraer la información pertinente, que nos permitirá analizar la viabilidad, en cuanto a la importancia, las necesidades e interés del tema en cuestión; y en tercera instancia se realizan las entrevistas y reuniones, que nos permitirán concretar el estudio, que justifica este proyecto.

Es necesario enfocar el proyecto en varias etapas o fases para asegurar que el estudio que justifica el proyecto, sea acorde a las necesidades de la FAC y al servicio educativo que se ofrece.

5.2 ESTRATEGIAS PARA LA INVESTIGACIÓN

Para el cumplimiento de los objetivos específicos, se manejó una estrategia de recolección y análisis de información, de acuerdo al orden de los objetivos planteados así: análisis de la formación integral del personal de la Fuerza Aérea Colombiana, para lograr identificar los fines de la educación impartida; que permitirán plantear una propuesta con un enfoque pedagógica. Análisis de los cursos que se dictan en ciberespacio, para ampliar y proyectar el estudio de la necesidad e importancia de formar personal calificado, para implementar, desarrollar y conducir operaciones en el ciberespacio, como una estrategia militar y así en las recomendaciones presentar el enfoque pedagógico, que debería implementarse en este campo del ciberespacio, con capacidades propias de la FAC.

Finalizada esta parte se realiza una encuesta, dirigida a los oficiales ,suboficiales y civiles que se puedan proyectar en este campo, con el fin de analizar la viabilidad en cuanto a conocimiento en ciberespacio, en importancia, necesidad e interés de formarse, para implementar, desarrollar y conducir operaciones en el ciberespacio, como una estrategia militar. y seguido se entrevistó a un personal de la jefatura de operaciones aéreas especializados en desarrollar y proyectar capacidades en el ciberespacio, a un personal de DITIN, Ingenieros de sistema, con experiencia o algún contacto con esta área y a un pedagogo; y además se entrevistó a algunos aspirantes a oficiales, propios de la carrera de ingeniería informática, con el fin de conocer las capacitaciones, instrucción, innovaciones educativas y tecnológicas entrenamiento las capacidades y proyecciones estratégicas de la Fuerza aérea en el campo de las operaciones en el ciberespacio.

Con toda esta información ya se justifica el proyecto y se plantean las recomendaciones y conclusiones, para dar solución a la problemática planteada.

5.2.1 Trayectos de las estrategias de investigación

A continuación se presenta el diseño de investigación que se aplicó, con el fin de exponer las tareas desarrollas para alcanzar los objetivos de estudio que permitirán contestar el interrogante planteado en la formulación del problema.

En tal sentido, se presentan los trayectos de estrategias de investigación como un Proceso de evaluación permanente interrelacionando las etapas de: recolección de información y datos (a través de la documentación, las encuestas y entrevistas), análisis, conclusión de la información y diseño.

Cuadro. 1 Trayectos de Estrategias de Investigación

Fases del proceso	**Propósito**
Primera	**Recolección de la información y estructura del proyecto**
Segunda	**Marco teórico, institucional, material y método**
Tercera	**Análisis de resultados y conclusiones**
Cuarta	**Revisión integral del texto del proyecto**
Quinta	**Preparación para la sustentación.**

Fuente: Parámetros ESDEGUE 2013

5.3 PROCEDIMIENTO DE LA ESTRATEGIA

5.3.1 Inicio

Para desarrollar esta investigación se cuenta con el apoyo de JOA, en cabeza del My Niño Andrés, JAL, en cabeza del Ct Ramírez Rojas Álvaro, Asesor internacionalista Henry Cancelado, DITIN, en cabeza de la Cr Deisy Garces-DITIN, en cabeza de la Cr Ramirez Patricia. Esta investigación de tipo aplicada, se

basa en instrumentos, como encuestas, entrevistas y reuniones con personal capacitado y con experiencia en este campo, el cual ayuda a presentar un estudio objetivo que justifica la propuesta, adecuada a las necesidades de la Fuerza Aérea Colombiana en Operaciones en el Ciberespacio.

Se logró reunir toda la documentación con la información pertinente y realizar el análisis, en reuniones en grupo y con los asesores temáticos, para ir cumpliendo los objetivos específicos, que llevo a alcanzar el objetivo general, de realizar un estudio que permita justificar la importancia y necesidad de formar personal calificado en implementar, desarrollar y conducir operaciones en el ciberespacio.

5.3.2 Población

Las personas para las cuales va dirigida esta encuesta, son los oficiales, suboficiales, civiles de la FAC, proyectados en este campo, pertenecientes a JOA, JIN y DITIN, los cuales son aproximadamente 200, para formar un grupo dedicado a implementar, desarrollar y conducir Operaciones en el Ciberespacio. Estas personas son las indicadas para resolver la encuesta, porque tendremos las opiniones de los entes interesados, según la delimitación que se hizo del proyecto; lo cual permitirá analizar mucho mejor la viabilidad en cuanto a importancia, necesidad e interés de las personas a las cuales va dirigido el proyecto; dando herramientas para el estudio en cuestión. La encuesta fue contestada por 143 personas, de los cuales 61 son oficiales activos y 55 suboficiales activos y 27 civiles activos

Según lo anterior se entiende que se escogió una población con unas características específicas, es decir el muestreo es selectivo y corresponde al 70% de la población aproximadamente.

Estas 143 encuestas escritas, se administraron durante las 2 últimas semanas de junio, del año en curso.

5.3.3 Instrumento

Como primer instrumento, para recolectar la información pertinente se contactó a las personas encargadas de JEA, IMA, ESINA, ESUFA, EMAVI, JOA, JIN, JAL, DITIN, que facilitaron la documentación y posteriormente una reunión con ellos, lo cual aclaro dudas y facilito el análisis de la información

Como segundo instrumento, se utilizó la encuesta de forma escrita que según Burke[61], se caracteriza por la recopilación de testimonio; lo cual permitió analizar la viabilidad en cuanto a importancia, necesidades e interés de formar personal calificado e idóneo en la implementación, desarrollo y conducción de operaciones en el ciberespacio.

El objetivo de la encuesta, que se quiere aplicar, es el de analizar la viabilidad de este proyecto en cuanto a importancia, necesidad e interés en formar personal calificado en la implementación, desarrollo y conducción de operaciones en el ciberespacio.

La pregunta 1 de la encuesta, busca medir si el término operaciones en el ciberespacio es conocido y se entiende su aplicación en la FAC.

La pregunta 2 de la encuesta, busca medir la experiencia que tiene el encuestado en operaciones en el ciberespacio, lo cual permite delimitar la encuesta a personas que han estado en este campo.

La pregunta 3 de la encuesta, busca conocer las capacitaciones a las cuales accede el personal de la FAC en el campo del ciberespacio-cibrnética y la relación

---

[61] PALLARES-BURKE, María. La nueva historia. Barcelona: editorial Universidad de Granada, 2005. p. 183.

que hay entre experiencia versus capacitación, lo cual permite delimitar aún más la encuesta.

La pregunta 4 de la encuesta es aún más directa, porque quiere conocer la opinión del encuestado, de si es importante que el personal de la FAC, sea capacitado para implementar, desarrollar y conducir operaciones en el ciberespacio; lo cual permite analizar viabilidad del proyecto otorgando herramientas claras para la justificación del estudio.

La pregunta 5 de la encuesta, también es muy directa, porque mide el interés del encuestado en formarse en esta área; lo cual es una motivación más y proporciona herramientas, para el estudio.

La pregunta 6 de la encuesta, permite analizar las consecuencias que traería para la FAC una formación completa y adecuada en operaciones en el ciberespacio; en cuanto al cumplimiento de su misión.

La pregunta 7 de la encuesta, busca que el encuestado se cuestione, en cuanto al perfil del oficial en la carrera militar, como comandante, ya sea del cuerpo de vuelo o no; para manejar los recursos y procesos enmarcados en operaciones en el ciberespacio; lo cual sigue dando herramientas para justificar el estudio.

Como tercer instrumento, fue la reunión final con un ingeniero de sistemas y especialista en ciberespacio y un oficial FAC, cuya especialidad es en defensa y seguridad de bases y que lleva dos años trabajando en este campo, y un pedagogo, para presentar un proyecto que permita implementar, desarrollar y conducir las operaciones en el ciberespacio; quienes contribuyeron a concluir y justificar el estudio.

5.3.4 Procesamiento de la información

Se logró el análisis de la información recolectada a través de las lecturas realizadas a la documentación entregada por: ESUFA, ESINA, EMAVI, JIN, JEA, JOA, DITIN y el comando, en las reuniones con las fuentes.

Con el resultado de las encuestas se procesaron cada una de las preguntas de manera estadística, como son medidas repetidas, se utiliza un "análisis estadístico"[62] utilizando frecuencias, a partir de una tabulación de los resultados, en Excel se obtuvieron las gráficas.

5.3.4.1 Gráficas de los resultados de la encuesta.

El número de las primera 7 gráficas corresponde al número de la pregunta, con sus respectivas tablas, porque se tabularon las encuestas de los oficiales, suboficiales, civiles versus cada pregunta. De la tabla 8 a la 11 se presentan los respectivos análisis cruzados, entre capacitación/ experiencia, Ciberespacio/ explicación operaciones en el ciberespacio, capacitación /cursos e importancia de la Formación/ explicación.

Pregunta 1. ¿Sabe usted que son operaciones en el ciberespacio?

Tabla 1. Grado Vs OCBS

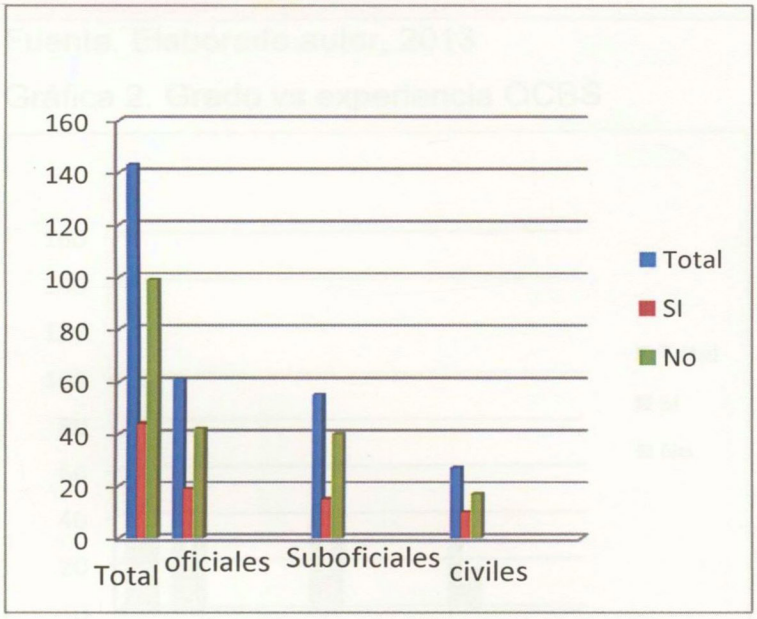
Observada Esperada Residuos Normalizados corregidos		SI	NO
	143	44 (30,8%)	99(69,2 %)

[62] MORE, David. Estadística aplicada básica. Barcelona, 2000. p. 510

Observada Esperada Residuos Normalizados corregidos		SI	NO
Oficial	61	19	42
Suboficial	55	15	40
Civil	27	10	17

Fuente. Elaborado por autor, 2013

Gráfica 1. Grado vs OCBS



Fuente. Elaborada autor, 2013

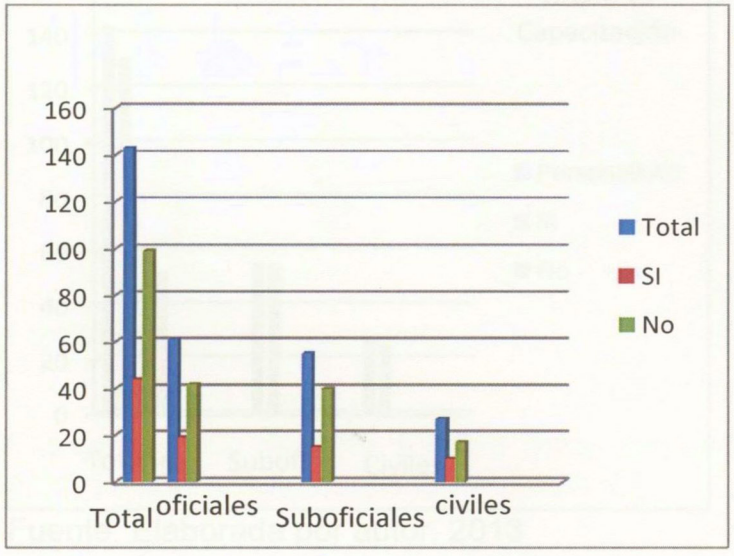
Pregunta 2. Su experiencia en tiempo para implementar, desarrollar y ejecutar operaciones en el ciberespacio es de.

Tabla 2. Grado vs experiencia OCBS

Observada Esperada Residuos Normalizados corregidos		Entre 1 y 5 años	Entre 5 y 10 años	Entre 10 y 20 años	No tengo experiencia
	143	10(7%)	3(2,1%)	1(0,7%)	129(90,2%)
Oficial	61	6	3	1	51
Suboficial	55	2	0	0	53
Civil	27	2	0	0	25

Fuente. Elaborado autor, 2013

Gráfica 2. Grado vs experiencia OCBS



Fuente. Elaborada por autor, 2013

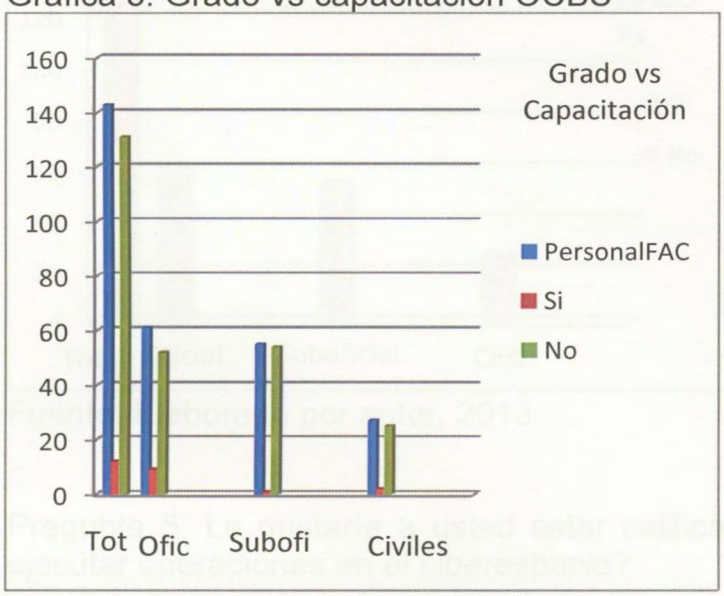
Pregunta 3. ¿Tiene alguna capacitación para implementar, desarrollar o ejecutar operaciones en el ciberespacio?

Tabla 3. Grado vs capacitación OCBS

Observada Esperada Residuos Normalizados corregidos		SI	NO
	143	12(8,4%)	131(91,6%)
Oficial	61	9	52
Suboficial	55	1	54
Civil	27	2	25

Fuente. Elaborada por autor, 2013

Gráfica 3. Grado vs capacitación OCBS



Fuente. Elaborada por autor, 2013

Pregunta 4. ¿Le parece a usted importante que el personal de la FAC, sea capacitado para implementar, desarrollar y ejecutar operaciones en el ciberespacio?

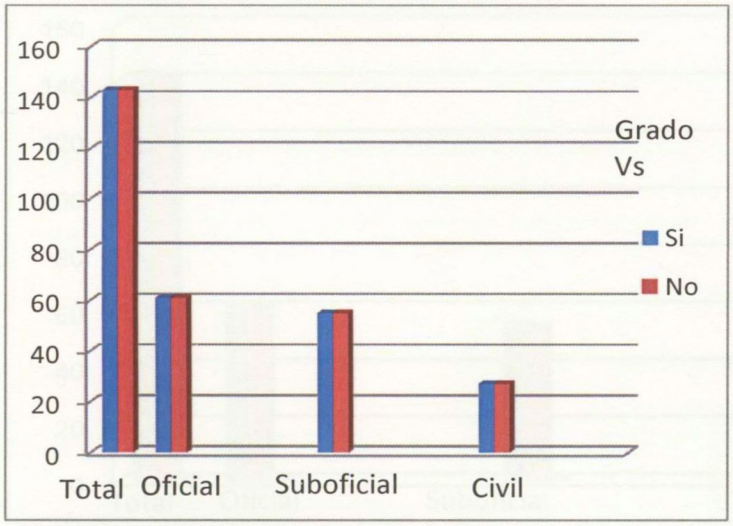
Tabla 4. Grado vs importancia OCBS

Observada Esperada Residuos Normalizados corregidos		SI

	143	143(100%)
Oficial	61	61
Suboficial	55	55
Civil	27	27

Fuente. Elaborada por autor, 2013

Gráfica 2. Grado Vs formación OCBS



Fuente. Elaborado por autor, 2013

Pregunta 5. Le gustaría a usted estar calificado para implementar, desarrollar y ejecutar operaciones en el ciberespacio?

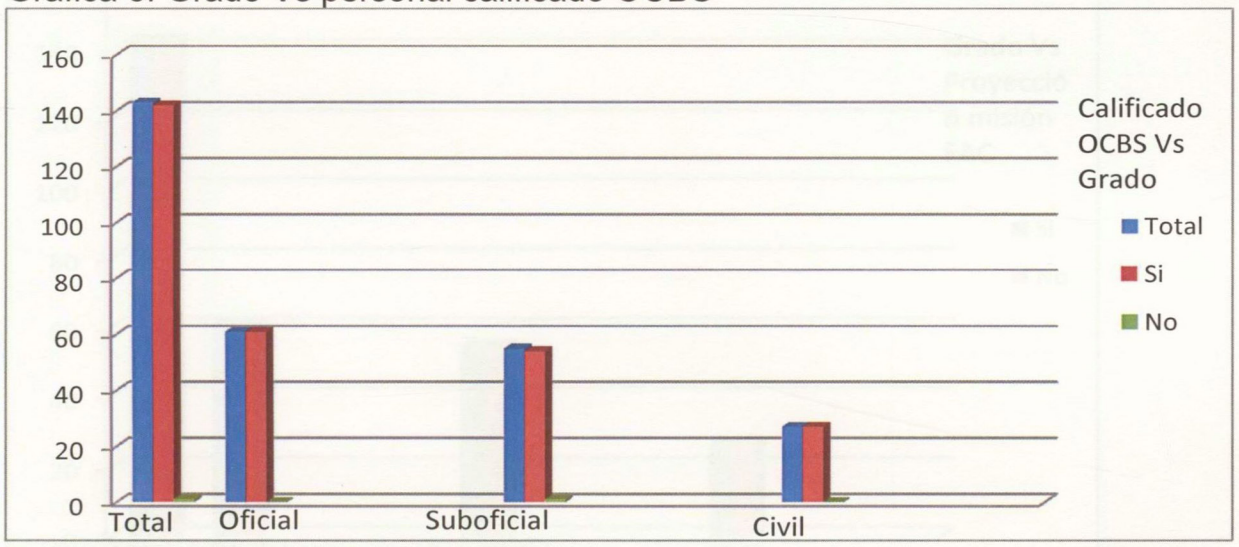
Tabla 5. Grado Vs calificado OCBS

Observada Esperada Residuos Normalizados corregidos		SI	NO
	143	142(99,3%)	1(0,75%)
Oficial	61	61	0

Observada Esperada Residuos Normalizados corregidos		SI	NO
Suboficial	55	54	1
Civil	27	27	0

Fuente. Elaborada por autor, 2013

Gráfica 3. Grado Vs personal calificado OCBS



Fuente. Elaborada por el autor, 2013

Pregunta 6. Considera usted que un personal capacitado, para implementar, desarrollar y ejecutar operaciones en el ciberespacio, contribuiría a proyectar la misión de la FAC?

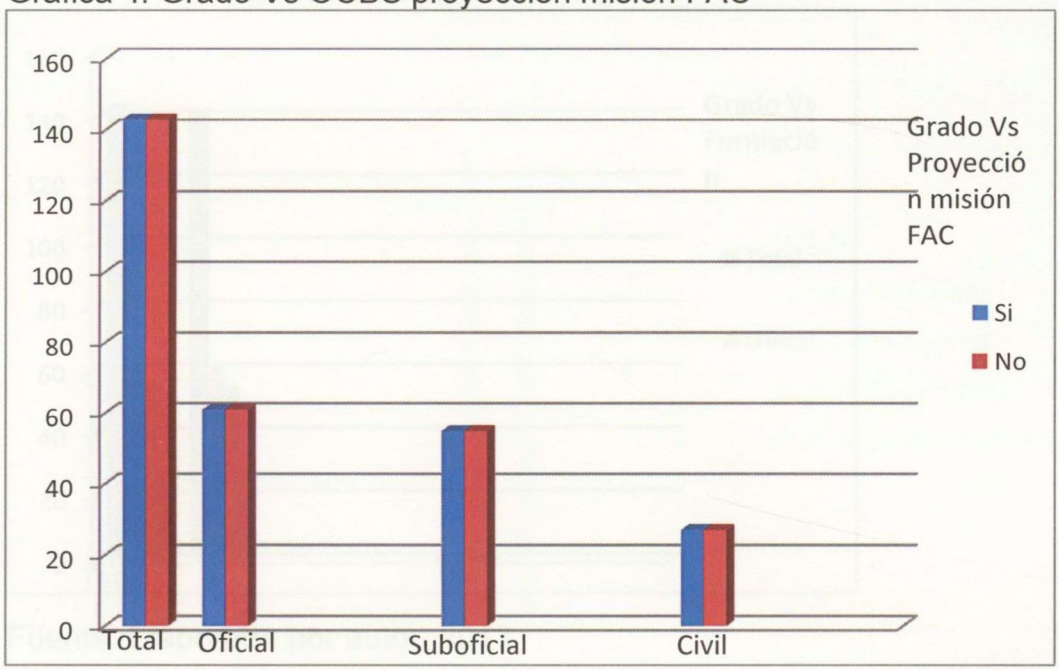
Tabla 6. Grado Vs OCBS proyección misión FAC

Observada Esperada Residuos Normalizados corregidos	Total	SI
	143	143
Oficial	61	61

Observada Esperada Residuos Normalizados corregidos	Total	SI
Suboficial	55	55
Civil	27	27

Fuente. Elaborada por autor, 2013

Gráfica 4. Grado Vs OCBS proyección misión FAC



Fuente. Elaborada por autor, 2013

Pregunta 7. ¿Cree usted que es importante y necesario, que los Oficiales tengan una formación idónea, para implementar, desarrollar y ejecutar operaciones en el ciberespacio y así, direccionar y orientar mejor los recursos humanos, técnicos y los procesos que abarquen este campo?

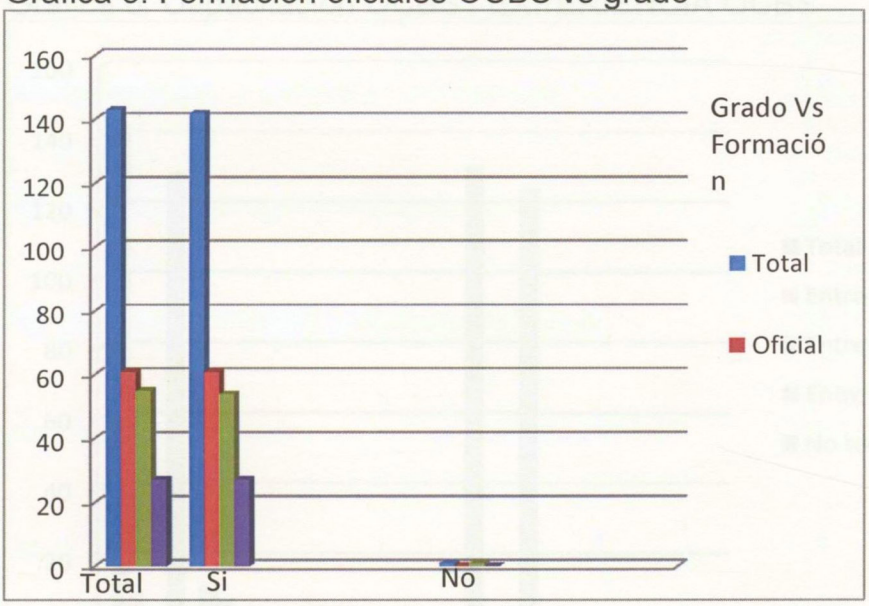
Tabla 7. Formación OFC OCBS Vs Grado

Observada Esperada Residuos Normalizados corregidos		Oficial	Suboficial	Civil
	143	61	55	27

Observada Esperada Residuos Normalizados corregidos		Oficial	Suboficial	Civil
SI	142	61	54	27
NO	1	0	1	0

Fuente. Elaborada por autor, 2013

Gráfica 5. Formación oficiales OCBS vs grado



Fuente. Elaborada por autor, 2013

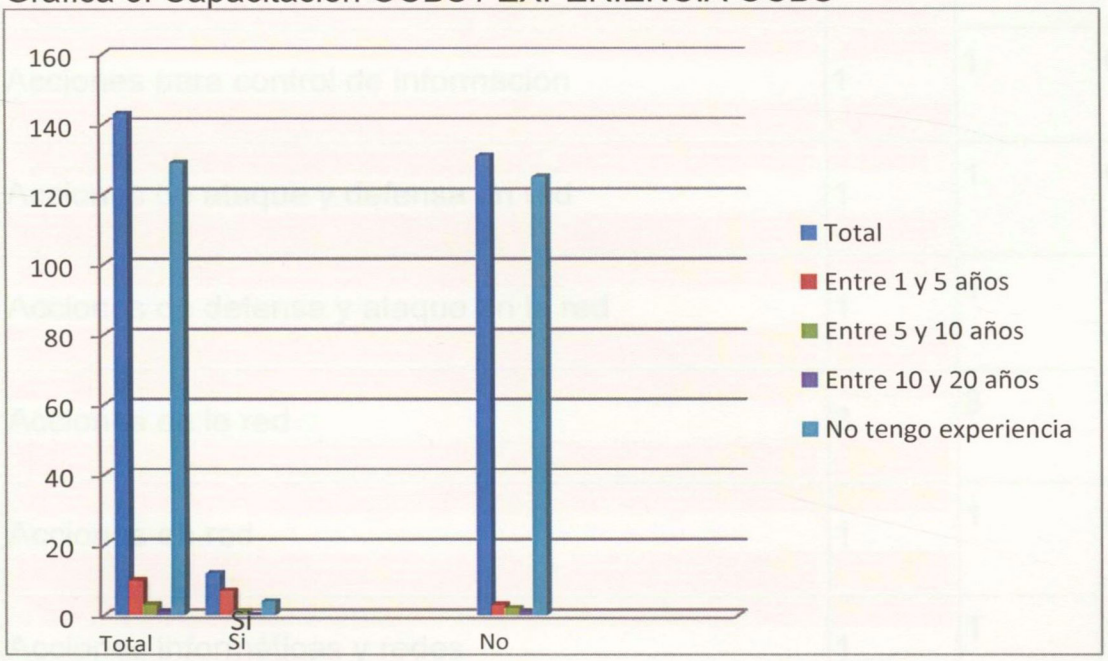
Tabla 8. Capacitación OCBS/experiencia OCBS

Observada Esperada Residuos Normalizados corregidos		Entre 1 y 5 años	Entre 5 y 10 años	Entre 10 y 20 años	No tengo experiencia
	143	10	3	1	129
SI	12	7	1	0	4

Observada Esperada Residuos Normalizados corregidos		Entre 1 y 5 años	Entre 5 y 10 años	Entre 10 y 20 años	No tengo experiencia
NO	131	3	2	1	125

Fuente. Elaborada por autor, 2013

Gráfica 6. Capacitación OCBS / EXPERIENCIA OCBS



Fuente. Elaborada por autor, 2013

Tabla 9. Explicación Ciberespacio-Ciberespacio

Observada Esperada Residuos Normalizados corregidos		SI	NO
	143	44	99
Acciones que usan el espectro electromagnético	1	1	0
Acciones para cuidar espacio virtual	1	1	0

Observada Esperada Residuos Normalizados corregidos		SI	NO
Acciones a nivel satelial	1	1	0
Acciones a través de la red	1	1	0
Acciones a través de la red	1	1	0
Acciones para control de informacion	1	1	0
Acciones de ataque y defensa en red	1	1	0
Acciones de defensa y ataque en la red	1	1	0
Acciones en la red	3	3	0
Acciones en red	1	1	0
Acciones informáticas y redes	1	1	0
Acciones informaticas	3	3	0
Actividad en la red	1	1	0
Actividades a traves de la red	1	1	0
Aprovechamiento del espacio electromagnético	1	1	0
Ataque y defensa en los sitios de informacion	1	1	0

Observada Esperada Residuos Normalizados corregidos		SI	NO
Dirigidas a ataques cibernéticos	1	1	0
Esrategias en la red	1	1	0
Estrategia a través de la red	1	1	0
Estrategias a nivel digital	1	1	0
Estrategias a traves de la red	1	1	0
Estrategias cibernéticas	1	1	0
Estrategias en la red	4	4	0
Estrategias en red	1	1	0
Estrategias para evitar vulnerabilidad en la información	1	1	0
Estrategias informáticas, aplicadas en la red	1	1	0
Estrategias que usan satelites	1	1	0
Estrategias tecnologicas	1	1	0
Estrategias en la red	1	1	0
Las cuales utilizan satelites	1	1	0

Observada Esperada Residuos Normalizados corregidos		SI	NO
Operacion entre las redes	1	1	0
Protección de información, cumplimiento de la misión FAC	1	1	0
Tecnologias en el aprovechamiento del 5to elemento	1	1	0
es una guerra informática	1	1	0
evita acciones ilícitas desde CS	1	1	0
manejo información digital	1	1	0
uso de 5 elementos	1	1	0
Ns/Nc	99	0	99

Fuente. Elaborada por autor, 2013

Tabla 20. Cursos capacitación OCBS/capacitación OCBS

Observada Esperada Residuos Normalizados corregidos		SI	NO

Observada Esperada Residuos Normalizados corregidos		SI	NO
	143	12	131
CGE	1	1	0
CH,MA,O	1	1	0
CVGE	2	2	0
ESI	1	1	0
H,SI,R,S	1	1	0
Ing Inf	4	4	0
P,R,M	1	1	0
Ns/Nc	132	1	131

Fuente. Elaborada por autor, 2013

Tabla 11. Por qué importancia OCBS/importancia OCBS

Observada Esperada Residuos Normalizados corregidos		SI
	138	138
Avances de la FAC	2	2

Observada Esperada Residuos Normalizados corregidos		SI
Avances de la fuerza	1	1
Capacidad	1	1
Prepararnos…Ciberguerra	1	1
Prepararnos..Ciberguerra	1	1
Crear doctrina	6	6
Crear doctrina en la FAC	3	3
Defensa	1	1
Desarrollo	13	13
Dominio aéreo- espacial	1	1
Evolución de la guerra	4	4
Evolución del conflicto	1	1
Evolución de la guerra	20	20
Evolución de la guerra	1	1

Observada Esperada Residuos Normalizados corregidos		SI
Exposición de la información	1	1 **
Futuro de la guerra	3	3 3 **
Futuro	5	5 5 **
Liderazgo	1	1 1 **
Necesidad	1	1 1 **
Otras entidades	1	1 1 **
Pioneros en Colombia	1	1
Pioneros en las fuerzas	1	1
PoderCBS	1	1
Prevención	1	1
Proyección FAC	1	1

Observada Esperada Residuos Normalizados corregidos		SI
Protección de la información	2	2
Proyección de la fuerza	3	3
Proyección	36	36
Proyectar la Vision FAC	1	1
VisionFAC	20	20
Vision de la FAC	2	2
Ns/Nc	1	1

Fuente. Elaborada por el autor, 2013

Estos resultados reflejan la importancia, necesidad e interés que tiene el ciberespacio y las operaciones que se puedan implementar, desarrollar y conducir allí, para el personal de la FAC, que se proyecte en este campo. Y es necesario e importante para el personal de la FAC proyectado en este campo estar calificado para implementar, desarrollar y conducir operaciones en el ciberespacio, en un 100%, lo evidencio la encuesta. Aunque es evidente que solo el 30.8%, de este personal tiene una explicación de ciberespacio y las operaciones que se puedan implementar, desarrollar y conducir a través de este medio, el 90,2% de este

personal de la FAC no tiene experiencia en implementar, desarrollar o conducir operaciones en el ciberespacio y el 91,6% no tiene capacitación para implementar, desarrollar y conducir operaciones en el ciberespacio; sin embargo hay un 1,4% que no tiene ninguna capacitación en este campo, pero ha adquirido experiencia.

Al 99,3% del personal encuestado le gustaría estar calificado para desarrollar, implementar y conducir operaciones en el ciberespacio y también este porcentaje cree que es importante y necesario que los oficiales tengan una formación idónea en este campo, para direccionar y orientar mejor los recursos humanos, técnicos y los procesos que abarquen las operaciones en el ciberespacio, contribuyendo a la misión de la FAC.

El 100% del personal encuestado, que se proyecte en este campo, considera que un personal calificado, para implementar, desarrollar y ejecutar operaciones en el ciberespacio, contribuiría a proyectar la misión de la FAC.

Al realizar la tabulación cruzada se evidencia que no hay un criterio unificado y claro de lo que son las operaciones en el ciberespacio y que las capacitaciones que se dictan son muy escazas, para un tema en el que la FAC debe ser pionero, igualmente el personal entrevistado cree que es importante tener personal calificado, por proyección, evolución de la guerra o conflicto y para contribuir a la visión de la FAC.

Todo el estudio realizado, demuestra que hay una viabilidad en cuanto a la importancia, necesidad e interés, lo que nos permite justificar la propuesta de formar personal calificado para la implementación, desarrollo y conducción de las operaciones en el ciberespacio, pero es necesario primero reglamentar la especialidad propia en este campo, ya que no está reglamentada, estructurando de quien puede depender, de una manera clara y objetiva, donde todo el personal proyectado en esta área, trabaje como un todo, en pro del desarrollo y proyección de la Fuerza, para salvaguardar la Seguridad Nacional(ver anexo B); segundo

realizar el estudio de los gastos económicos y la malla curricular, que se puede implementar, basándose en otras entidades extranjeras y nacionales; iniciando con formación tecnológica, propia para los suboficiales, de pregrado para los oficiales, orientada hacia el liderazgo que deben tener los oficiales, para direccionar todos los recursos utilizados en los procesos en este campo y los que deseen profesionalizarse y estudios de posgrado, como especializaciones, maestria y porque no doctorado; además de cursos de formación, como capacitaciones o entrenamientos, ya que se ha evidenciado que la FAC se preocupa por la preparación de su personal y así poder cumplir con su misión. Es claro que este proyecto en sí justifica la propuesta de la importancia y necesidad de formar personal calificado en implementar, desarrollar y conducir las operaciones en el ciberespacio.

Por lo cual la propuesta es organizar un eje temático bien estructurado, para formar un plan de estudios, acorde a un plan de carrera, adecuado a oficiales, suboficiales y civiles de la FAC. Donde se parte de un conocimiento básico, igual para todas las carreras aquí planteadas y que se ampliara de acuerdo al plan de estudio que se impartirá, para una formación tecnológica y de pregrado; lo cual será el conocimiento intermedio, ya el conocimiento avanzado lo da el plan de estudios de la carrera de postgrado. Además también se pueden implementar capacitaciones que incluyen entrenamientos, para mantener al personal de la FAC actualizado. Y así recibir una formación basada en un eje articulado que permita trabajar en equipo.

Esta es solo una propuesta justificada por el estudio que se hizo de la importancia de formar personal calificado, en la FAC, para la implementación, desarrollo y conducción de operaciones en el ciberespacio.

FORMAR PERSONAL CALIFICADO PARA LAS OPERACIONES EN EL CIBERESPACIO.

OBJETIVO: Formar integralmente al personal dando herramientas claras, objetivas y precisas, para estandarizar la implementación, desarrollo y conducción de las operaciones en el ciberespacio y así mantener el poder aéreo-espacial en pro de la Seguridad Nacional.

DIRIGIDO: A todo el personal de la FAC que se proyecte en el campo del ciberespacio, JIN, JOA, DITIN, para así potencializar sus capacidades y para otras fuerzas nacionales o internacionales.

CONTENIDO: La propuesta de formar personal calificado en este campo abarca:

La implementación de una carrera tecnología, para los suboficiales enfocada al manejo de las innovaciones tecnológicas que surjan en este campo.

La implementación de una carrera de pregrado, para los oficiales, pero enfocada hacia el diseño de estrategias, para el liderazgo, manejo y direccionamiento de los recursos en este campo del ciberespacio, que deben tener los oficiales.

La implementación de una carrera de postgrado, enfocada a la investigación de tecnologías y estrategias que potencialicen aún más las capacidades en este campo, como una estrategia militar en pro de la seguridad Nacional.

La implementación de cursos de formación, que incluyan capacitaciones y entrenamiento, para los civiles y demás personal proyectado, que mantenga a la FAC a la vanguardia en este campo del ciberespacio, para la conducción de operaciones.

LOS EJES TEMÁTICOS. Para direccionar los contenidos en los procesos Enseñanza-Aprendizaje, se propone tener en cuenta los siguientes ejes en cada carrera.

1. Ciberespacio: conocimiento amplio de acuerdo a las necesidades que exija cada carrera, obviamente se parte de un conocimiento básico. Donde se pueda contar con personal experto en perimetrales, intrusión, virología y contingencia.

Contenido básico: Introducción a las operaciones en el ciberespacio, Fundamentos: de tecnologías de información, de operaciones de despliegue, de redes IP, de redes de misiles y satelitales, de sistemas de control industrial, de defensa y protección de redes, de programación segura, de criptografía, de seguridad de la información.

2. Psicología: liderazgo para el direccionamiento del recurso humano en los procesos de este campo.

3. Administración: manejo de los recursos en los procesos propios de esta área.

4. Relaciones Políticas y asuntos Internacionales: manejo de las relaciones que contribuyan a potencializar los procesos propios de este campo.

5. Investigación: parámetros claros para la implementación y desarrollo de nuevas tecnologías, que permitan estar a la vanguardia en el campo del ciberespacio y las operaciones que se puedan conducir allí; en pro de la Seguridad Nacional.

ALCANCE: Formar personal idóneo propio del campo del ciberespacio, para la implementación, desarrollo, conducción y ejecución de las operaciones a través del ciberespacio; proyectando así la misión y visión de la FAC.

CONCLUSIONES

Para el personal de la Fuerza Aérea Colombiana, que se proyecta en el campo del ciberespacio, para implementar, desarrollar y conducir operaciones a través de este medio, es muy importante y necesario capacitarse, como ciberguerreros porque les permite adquirir una formación más amplia, oportuna y precisa en este campo. Con el fin de potencializar sus capacidades, en el manejo de innovaciones tecnológicas, en el diseño de estrategias, más efectivas y certeras, al direccionar y liderar los recursos humanos y técnicos en los procesos concernientes a esta área, que aún está poco explotada y que requiere de toda la proyección en la fuerza, para controlar y mantener el poder aéreo-espacial. Aprovechando la infraestructura que tiene la FAC a nivel educativo y su preocupación por estar a la vanguardia en innovaciones tecnológicas y educativas. Para así lograr resultados positivos y mejor direccionados en pro de la Seguridad Nacional, que es un objetivo primordial de la Fuerza Aérea.

Para el personal de aspirantes a oficiales de la Fuerza Aérea Colombiana, que adelanta sus estudios en la Escuela Militar de Aviación, Marco Fidel Suarez, es muy interesante la propuesta, ya que les gustaría adquirir la formación superior en el diseño de estrategias, para liderar y direccionar los recursos humanos y técnicos con un mayor grado de idoneidad e irlos perfeccionando a lo largo de su carrera profesional, como militares. Contribuyendo así, a lograr resultados positivos y mejor direccionados en pro de las operaciones en el ciberespacio en el marco de la Seguridad Nacional, que es un objetivo primordial de la Fuerza Aérea.

Es evidente que para la Fuerza Aérea Colombiana, es muy importante la formación integral de su personal y más aún en este campo, para la implementación, desarrollo y conducción de las operaciones en el ciberespacio. Sin embargo, aunque cuenta con la infraestructura necesaria para abrirse en este campo del ciberespacio, aún no hay nada implementado a nivel educativo, propio de la fuerza, para lo cual debería ser pionera. Es por eso, que es viable la

implementación de la formación en este campo, para el personal proyectado, con el propósito de formar líderes, capaces del manejo de innovaciones tecnológicas y el diseño de estrategias; que permitan implementar, desarrollar y conducir operaciones en el ciberespacio, en pro de la visión institucional.

Al formar personal calificado o mejor aún cualificado en la implementación, desarrollo y conducción de las operaciones a través del ciberespacio, se potencializan las capacidades, de los ciberguerrero, en este campo, lo que favorece la estrategia militar. Ya que permite que los oficiales se formen como líderes, capaces de diseñar estrategias, para la formulación de planes de ciberdefensa Nacional en tiempo de paz y operaciones militares, ciberataque, en tiempo de guerra. Por lo tanto en cabeza de este personal, se debe producir el conocimiento vital para la supervivencia nacional; en respuesta al acelerado crecimiento tecnológico y del cual no podemos escapar y debemos ser pioneros y a interrogantes relacionados con la fuerza de ciberguerreros antagónicos, sus intenciones y apreciación de las probables respuestas a los actos, por estos proyectados.

La metodología utilizada en el desarrollo de esta investigación, permitió alcanzar los objetivos propuestos, dando solución a la problemática planteada; lo cual se evidencio a través del análisis de los resultados de la encuesta y los demás instrumentos utilizados. Proporcionando datos que justifican la importancia y la necesidad de formar personal calificado, mejor aún cualificado, ciberguerreros, para implementar, desarrollar y conducir operaciones en el ciberespacio, como una estrategia militar, en la ciberguerra. En pro de potencializar capacidades de liderazgo que permitan el manejo de nuevas tecnologías y el diseño de estrategias; que direccionen los recursos humanos y técnicos, en los procesos de este campo del ciberespacio.

A través del análisis y evaluación de los resultados de este proyecto de investigación, se logró identificar las necesidades, falencias e intereses que tiene la Fuerza Aérea Colombiana en el campo del ciberespacio; justificando así, la importancia e interés de formar personal calificado, para implementar, desarrollar y conducir operaciones a través de este medio; lo cual permitirá fortalecer el proceso militar en la toma de decisiones, como herramienta indispensable y decisiva en el direccionamiento de los objetivos nacionales, además de proyectar a la Fuerza en un campo en el cual debe ser pionera. Porque aunque finalice con éxito el proceso de paz, siempre surgirán grupos subversivos que no están de acuerdo con el estado y seguramente ataquen, utilizando otras armas y medios tecnológicamente más avanzados, donde cabe el concepto de ciberespacio y ciberguerra.

Por lo cual la propuesta es organizar un eje temático bien estructurado, para formar un plan de estudios, acorde a un plan de carrera, adecuado a oficiales, suboficiales y civiles de la FAC. Donde se parte de un conocimiento básico, igual para todas las carreras aquí planteadas y que se ampliara de acuerdo al plan de estudio que se impartirá, para una formación tecnológica y de pregrado; lo cual será el conocimiento intermedio, ya el conocimiento avanzado lo da el plan de estudios de la carrera de postgrado. Además también se pueden implementar capacitaciones que incluyen entrenamientos, para mantener al personal de la FAC actualizado. Y así recibir una formación basada en un eje articulado que permita trabajar en equipo.

Esta es solo una propuesta justificada por el estudio que se hizo de la importancia de formar personal calificado, en la FAC, para la implementación, desarrollo y conducción de operaciones en el ciberespacio.

RECOMENDACIONES

Formar un grupo especial, que se dedique a implementar, desarrollar y conducir operaciones en el ciberespacio, contando con personal que se proyecte desde la escuela de formación Marco Fidel Suarez y ESUFA, pero unificando los esfuerzos de toda la fuerza y reglamentar la especialidad en ciberespacio(ver anexo B).

Realizar el estudio de los gastos económicos y la malla curricular, que se puede implementar, en el plan de carrera, para el personal que se proyecte en esta área; teniendo en cuenta que los procesos de formación para los oficiales, suboficiales y civiles, deben ser direccionados de acuerdo a su desempeño y cumplimiento de funciones en la Fuerza.

FORMAR PERSONAL CALIFICADO PARA LAS OPERACIONES EN EL CIBERESPACIO.

OBJETIVO: Formar integralmente al personal dando herramientas claras, objetivas y precisas, para estandarizar la implementación, desarrollo y conducción de las operaciones en el ciberespacio y así mantener el poder aéreo-espacial en pro de la Seguridad Nacional.

DIRIGIDO: A todo el personal de la FAC que se proyecte en el campo del ciberespacio, JIN, JOA, DITIN, para así potencializar sus capacidades y para otras Fuerzas nacionales o internacionales.

CONTENIDO: La propuesta de formar personal calificado en este campo abarca:

- La implementación de una carrera tecnológica, para los suboficiales enfocada al manejo de las innovaciones tecnológicas que surjan en este campo.

- La implementación de una carrera de pregrado, para los oficiales, pero enfocada hacia el diseño de estrategias, para el liderazgo, manejo y direccionamiento de los recursos en este campo del ciberespacio, que deben tener los oficiales y que además permita la profesionalización del personal proyectado en este campo, que tenga la experiencia y cuente con cursos de formación, como capacitaciones y entrenamientos.
- La implementación de una carrera de postgrado, enfocada a la investigación de tecnologías y estrategias que potencialicen aún más las capacidades en este campo, como una estrategia militar en pro de la seguridad Nacional.
- La implementación de cursos de formación, que incluyan capacitaciones y entrenamiento, para los civiles y demás personal proyectado, que mantenga a la FAC a la vanguardia en este campo del ciberespacio, para la conducción de operaciones.

LOS EJES TEMÁTICOS. Para direccionar los contenidos en los procesos Enseñanza-Aprendizaje, se propone tener en cuenta los siguientes ejes en cada carrera.

1. Ciberespacio: conocimiento amplio de acuerdo a las necesidades que exija cada carrera, obviamente se parte de un contenido básico, para todas las carreras, enmarcadas en ciberespacio. Donde se pueda contar con personal experto en perimetrales, intrusión, virología y contingencia.

Contenido básico: Introducción a las operaciones en el ciberespacio, Fundamentos: de tecnologías de información, de operaciones de despliegue, de redes IP, de redes de misiles y satelitales, de sistemas de control industrial, de defensa y protección de redes, de programación segura, de criptografía, de seguridad de la información.

2. Psicología: liderazgo para el direccionamiento del recurso humano en los procesos de este campo.

Contenido básico: en leyes y ética del ciberespacio.

3. Administración: manejo de los recursos en los procesos propios de esta área.

4. Relaciones Políticas y asuntos Internacionales: manejo de las relaciones que contribuyan a potencializar los procesos propios de este campo.

5. Investigación: parámetros claros para la implementación y desarrollo de nuevas tecnologías, que permitan estar a la vanguardia en el campo del ciberespacio y las operaciones que se puedan conducir allí; en pro de la Seguridad Nacional.

ALCANCE: Formar personal idóneo propio del campo del ciberespacio, para la implementación, desarrollo, conducción y ejecución de las operaciones a través del ciberespacio; proyectando así la misión y visión de la FAC.

Es necesario, definir por parte de la Fuerza Aérea Colombiana, claramente que es una especialidad y cuáles son los requisitos para acceder a ella, concretamente en ciberespacio, lo cual es vital para su adecuado funcionamiento; donde cada integrante, allí proyectado, tenga claridad sobre sus funciones y se forme realmente un verdadero equipo, unificado; con ciberguerreros cualificados y comprometidos, y comandantes idóneos capaces de liderar y direccionar este personal a su mando.

Iimplementar cada una de las carreras: tecnología, pregrado, postgrado, enmarcadas en operaciones en el ciberespacio, con un nombre que se pueda proyectar fuera del campo militar y cursos de formación, los cuales incluyen capacitaciones y entrenamiento, según las necesidades de la FAC; en las

escuelas de formación que correspondan, según la organización educativa de la FAC.

Se tenga en cuenta la propuesta aquí presentada para que no se empiecen a implementar capacitaciones y entrenamientos no articulados a un eje temático claro, que busca formar personal cualificado en intrusión, perimetrales, virología y contingencia; lo cual permitirá que se implementen, desarrollen y conduzcan operaciones en el ciberespacio, de forma certera y optima, con comandantes que sean capaces de direccionar y liderar todos los recursos y procesos en este campo, en pro de la Seguridad Nacional.

BIBLIOGRAFÍA

AIR & SPACE, Power. Cyber warfare, USAF. Alabama, 2013.

BUCCI, Steven. Individual ciber-preparación es la defensa civil del siglo 21. The heritagefundation. Washington D.C. 2012.

CASTRO Reynoso, Sergio. Arquitectura de seguridad informática, Charleston sc. USA. 2013.

ECHAVARRIA BARRIENTOS, Raúl. En la ruta de las Estrellas, Libro de Oro, EMAVI. Cali, 1983.

FUERZA AÉREA COLOMBIANA, Manual de Calidad Versión 3, código FAC-DMC. Numeral 4.2.1.2.1, *Proceso Misional Inteligencia Aérea*.

FUERZA AÉREA COLOMBIANA. MANUAL DE DOCTRINA BÁSICA AÉREA Y ESPACIAL, Bogotá. Cuarta Edición. 2013

FUERZA AEREA COLOMBIANA, Manual de Inteligencia Aérea (O-INTAE) FAC 2-05 Reservado, junio de 2006.

FUERZA AÉREA COLOMBIANA, *Manual de operaciones de Inteligencia Aérea.* Bogotá, Fuerzas Militares(2da Edicion-055), 2010.

FUERZA AÉREA COLOMBIANA, *Manual de operaciones de Inteligencia Aérea.* Bogotá, Fuerzas Militares, 2010.

FUERZA AÉREA COLOMBIANA. Plan estrategico institucional2011-2030, Bogotá. 2011.

FUERZA AÉREA COLOMBIANA, *Vocación de victoria*. Bogotá, 2005.

FUERZA AÉREA COLOMBIANA., Resolución 212 del 2012, Articulo 1, Decreto 1495/02 y 4494/05.Bogotá(República de Colombia), 2012.

FUERZAS MILITARES DE COLOMBIA, *PIC, Cacom 6*. Tres Esquinas, Caquetá, 2008.

FUERZAS MILITARES DE COLOMBIA, *PIC, Comando Fuerza Aérea*. Bogotá, 2011.

FUERZAS MILITARES DE COLOMBIA, *PIC, Comando Fuerza Aérea*. Bogotá, 2012.

Historia del Internet [En línea] Disponible en: http://ciberespacio-total.blogcindario.com/2010/09/00001-ciberespacio-historia-del-internet-glosario-relacionado-al-tema-otros-etc-actividad-n-1.html Citado el 22 de marzo de 2012.

Ley 1288, Capítulo IV, Artículo 18 Centros de protección de datos de Inteligencia y Contrainteligencia; Artículo 19 Objetivos de los CPD; Artículo 20 Difusión de datos de inteligencia y Contrainteligencia.

Manual de Inteligencia y operaciones Aéreas, Artículo 4. Límites y fines de las actividades de Inteligencia y Contrainteligencia.

Manual de Inteligencia y operaciones Aéreas, Artículo 5. Principios de la Actividad de Inteligencia y Contrainteligencia.

MONTERO, David. El arte de la guerra, Intelligence segurity. USA.2011.

MINISTERIO DE DEFENSA NACIONAL COMANDO GENERAL FUERZAS MILITARES, *Inteligencia Estratégica*(2da Edición). Bogotá, 2000.

MINISTERIO DE DEFENSA. *Memorias al Congreso 2001-2002*. Bogotá (República de Colombia), Agosto de 2002.

MINISTERIO DE DEFENSA, Dirección de estudios sectoriales. Dirección de programas, Bogotá. 2009.

MORE, David . *Estadística aplicada básica*. Barcelona, 20002.

NEWSLETTER, IA. Army, Navy, Air forcé, and cyber-is it time for a cyberwarfare Branch of military. Washington D.C.2009. Vol 12. No 1.

NEWSLETTER, IA. Army, Navy, Air forcé, and cyber-is it time for a cyberwarfare Branch of military. Washington D.C.2009. Vol 12. No 2.

RODRIGUEZ GAITAN, Andrés. El ciberespacio. ESDEGUE. 2012.

PALLARES-BURKE María. *La nueva historia*. editorial Universidad de Granada, 2005.

QUINTERQ, Sirio. El arquitecto y la guerra de quinta generación, El sudamericano. México. D.C. 2011.

SANCHEZ Medero, Gema. En: Revista Política y Estrategia N° 114 – 2009.

ANEXO A

FUERZAS MILITARES DE COLOMBIA
ESCUELA SUPERIOR DE GUERRA

Encuesta acerca de la importancia, necesidad e interés de formar personal calificado en la Fuerza Aérea Colombiana, para implementar, desarrollar y conducir operaciones en el ciberespacio.

OBJETIVO: Recopilar información que permita desarrollar el proyecto de grado, requisito para el curso de ascenso de Estado Mayor, CEM 2013.

Cargo: _____

Grado:_____

ORIENTACIÓN DE LA ENCUESTA: a continuación se presenta un conjunto de preguntas que busca recopilar la opinión, en cuanto a la importancia, necesidad e interés de formar personal calificado en la Fuerza Aérea Colombiana, para implementar, desarrollar y conducir operaciones en el ciberespacio.

La encuesta está orientada a: Oficiales, suboficiales, civiles de la Fuerza Aérea Colombiana.

1. ¿Sabe usted que son operaciones en el ciberespacio?

SI	NO

Si contesto si explique: _____

2. Su experiencia en tiempo para implementar, desarrollar y ejecutar operaciones en el ciberespacio es de.

Entre 1 y 5 años
Entre 5 y 10 años
Entre 10 y 20 años
No tengo experiencia

3. ¿Tiene alguna capacitación para implementar, desarrollar o ejecutar operaciones en el ciberespacio?

SI NO

Si contesto si menciónelas: _____

_____

4. ¿Le parece a usted importante que el personal de la FAC, sea capacitado para implementar, desarrollar y ejecutar operaciones en el ciberespacio?

SI NO

Por qué? _____

_____

5. ¿Le gustaría a usted estar calificado para implementar, desarrollar y ejecutar operaciones en el ciberespacio?

SI	NO

6. ¿Considera usted que un personal capacitado, para implementar, desarrollar y ejecutar operaciones en el ciberespacio, contribuiría a proyectar la misión de la FAC?

SI	NO

7. ¿Cree usted que es importante y necesario, que los Oficiales tengan una formación idónea, para implementar, desarrollar y ejecutar operaciones en el ciberespacio y así, direccionar y orientar mejor los recursos humanos, técnicos y los procesos que abarquen este campo?

SI	NO

ANEXO B

Resoluciones que reglamentan las especialidades existentes en la FAC.

JURDH	
JED	
JEMFA	

REPÚBLICA DE COLOMBIA

FUERZA AÉREA

RESOLUCIÓN 212 DEL 2012

(04 ABR. 2012)

"Por la cual se adiciona y aclara la Resolución Nº 666 del 12 de octubre de 2011"

EL COMANDANTE DE LA FUERZA AÉREA COLOMBIANA

En uso de sus atribuciones legales y en especial la estipulada en el artículo 26 literal "C" del Reglamento de Publicaciones Militares, y

CONSIDERANDO:

Que mediante Resolución Nº 666 del 12 de octubre de 2011, se modificó la Resolución 366 del 16 de julio de 2007, adoptando las siglas de especialidades del personal militar de la Fuerza Aérea Colombiana, y designando la Jefatura o área funcional para cada área de conocimiento.

Que para efectos del planeamiento y control del potencial humano de la Fuerza Aérea Colombiana, es necesario establecer las siglas correspondientes a los cuerpos y especialidades del personal militar, así como las áreas de conocimiento, profesiones o modalidades técnicas profesionales o tecnológicas del personal militar, incluyendo aquellas que no fueron contempladas en la Resolución Nº 666 del 12 de Octubre de 2011.

Teniendo en cuenta las necesidades de la Fuerza Aérea Colombiana es indispensable actualizar las especialidades y áreas del conocimiento donde se incluyen las profesiones o modalidades tecnológicas o técnicas profesionales del personal militar.

En mérito de lo expuesto,

RESUELVE:

ARTÍCULO 1º. Aclarar y adicionar las siglas, área funcional de las especialidades y áreas de conocimiento de los Oficiales de la Fuerza Aérea Colombiana, así:

CLASIFICACIÓN GENERAL Decreto Ley 1790/00 - Modificado Ley 1104/2006	ESPECIALIDAD Dec. 1495/02 Dec. 4494/05	ÁREA DE CONOCIMIENTO	SIGLA	ÁREA FUNCIONAL
CUERPO DE VUELO	Pilotos	Pilotos	VPI	JOA
	Especialistas de vuelo	Defensa Aérea	VDA	
		Navegante	VNA	
		Inteligencia Técnica Aérea	VIA	JIN
CUERPO SEGURIDAD Y DEFENSA DE BASES AÉREAS	Inteligencia	Inteligencia Terrestre	SDI	JIN
		Contrainteligencia		
	Defensa de Bases Aéreas	Seguridad, Custodia y Vigilancia	SDB	JES
		Seguridad Física		
		Operaciones Aéreas Especiales		
		Explosivos		
		Armamento Terrestre y Equipo Especial		
		Caninos Militares		

JURDH	
JED	
JEMFA	

212 04 ABR. 2012

RESOLUCIÓN NÚMERO _____ DE _____ HOJA Nº

Continuación de la Resolución "Por la cual se adiciona y aclara la Resolución Nº 666 del 12 de octubre de 2011, adoptando unas siglas de especialidades del personal militar de la Fuerza Aérea Colombiana, y se designa la Jefatura o Área funcional para cada Área de Conocimiento"

CUERPO LOGÍSTICO AERONÁUTICO	Abastecimiento Aeronáutico	Logística Aeronáutica	LABA	JOL
	Armamento Aéreo		LARA	
	Mantenimiento Aeronáutico		LMAA	
	Telecomunicaciones		LTEL	
		Servicios a la Navegación Aérea	LTEL	JOA
		Ingenierías de Sistemas o Informáticos	LATE	JAL
	Administración Aeronáutica	Administración	LADA	
		Arquitecturas e Ingenierías de Apoyo Logístico		
		Comunicación Social		
		Matemáticas y Ciencias Naturales		
		Financieras		
		Gestión Tecnológica		JEA
		Áreas de la Educación		
CUERPO ADMINISTRATIVO	Ciencias de la Salud	Bacteriología	ASBA	DISAN
		Enfermería Superior	ASEJ	
		Medicina	ASMG	
		Fonoaudiología	ASFO	
		Odontología	ASOD	
		Ingeniería Biomédica/Bioingeniería	AIBI	
		Administración Hospitalaria y/o Salud	AAAH	
		Instrumentación Quirúrgica	ASIQ	
		Trabajo Social	ASTS	JEB
		Psicología	ASPC	IGEFA
		Higiene y Seguridad Industrial	ASHS	
		Salud Ocupacional	ASSO	
		Veterinaria	ASVE	JES
	Derecho y Ciencias Políticas	Derecho	ADER	JURDH
		Ciencias Políticas	ADCP	JIN
		Relaciones Internacionales	ADRI	
		Sociología	ADSO	
	Economía, Administración y Contaduría	Mercadotecnia	AAMT	JAL
		Administración de Empresas	AAAE	
		Administración Pública	AAAP	
		Contaduría y Afines	AACP	
		Ingeniería Financiera	AAIF	
		Administración Logística	AAAL	
		Economía	AAEC	
		Comercio Exterior y/o Internacional	AACX	JOL
	Ciencias Religiosas	Presbítero	ARPR	JED
	Ingeniería y Arquitectura	Arquitectura	AIAR	JAL
		Ingeniería Ambiental	AIAM	
		Ingeniería Catastral	AICA	
		Ingeniería Civil	AICI	
		Ingeniería de Sistemas o Informática	AISI	
		Ingeniería Eléctrica	AIEL	
		Ingeniería Logística	AILO	

		Ingeniero Agrónomo	AIGR	
		Ingeniería Forestal	AIFO	
		Ingeniería Nuclear	AINU	
		Ingeniería Sanitaria	AIBA	
		Ingeniería de Transportes y Vías	AITV	
		Ingeniería Topográfica	AITO	
		Ingeniería Electromecánica	AIEM	
		Ingeniería Electrónica	AIET	JOL
		Ingeniería Industrial	AIIN	
		Ingeniería Mecánica	AIME	
		Ingeniería Metalúrgica	AIMT	
		Ingeniería Química	AIQU	
		Ingeniería Aeronautica	AIAE	
		Ingeniería Mecatrónica	AIMC	
		Ingeniería Aeroespacial	AIAP	
		Ingeniería de Redes y Telecomunicaciones	AIRT	
	Comunicación Social	Comunicación Social y Periodismo	ACSP	JAL
	Ciencias de la Educación	Administración Educativa y Afines	AEAE	JEA
		Historia	AEHI	
		Licenciaturas y Afines	AELA	
		Docencia Universitaria	AEDU	
		Psicopedagogía	AEPS	
		Educación Física y Deportes	AEFD	
		Investigación	AEIN	
	Matemáticas y Ciencias Naturales	Matemáticas	AMMA	
		Estadística	AMES	JAL
		Ecología	AMEC	IGEFA
CUERPO JUSTICIA PENAL MILITAR		Derecho	CJPM	DEJUM

ARTÍCULO 2o. Aclarar y adicionar las siglas, área funcional de las especialidades y áreas de conocimiento de los Suboficiales de la Fuerza Aérea Colombiana, así:

CLASIFICACIÓN GENERAL Dec. Ley 1790/00 Modificado Ley 1104/2006	ESPECIALIDAD Dec. 1495/02 Disposición CGFM 043/2005	ÁREA DE CONOCIMIENTO	SIGLA	ÁREA FUNCIONAL
CUERPO TÉCNICO AERONÁUTICO	Abastecimiento Aeronáutico	Centros Logísticos, Adquisiciones Aeronáuticas, Comercio Exterior y Combustible de Aviación	TAB	JOL
	Comunicaciones Aeronáuticas	Defensa Aérea	TDA	JOA
		Servicios a la Navegación Aérea	TNA	
		Vuelos Especiales	TVE	
		Inteligencia Técnica Aérea	TIA	JIN
	Electrónica Aeronáutica	Mantenimiento Sistemas de Aviónica	TSA	JOL
		Mantenimiento Sistemas de Armamento Aéreo	TAA	
		Mantenimiento Equipo Electrónica Terrestre	TET	
		Mantenimiento Radares Terrestres	TRD	
	Mantenimiento Aeronáutico	Mantenimiento General Aeronaves	TMG	

JURDH	
JED	
JEMFA	

212 04 ABR. 2012

RESOLUCIÓN NÚMERO _____ DE _____ HOJA Nº _____

Continuación de la Resolución "Por la cual se adiciona y aclara la Resolución Nº 666 del 12 de octubre de 2011, adoptando unas siglas de especialidades del personal militar de la Fuerza Aérea Colombiana, y se designa la Jefatura o Área funcional para cada Área de Conocimiento"

		Estructuras Metálicas y Compuestas	TEM	
		Equipo Terrestre de Apoyo Aeronáutico	TTA	
		Aeroindustrial	TAI	
CUERPO TÉCNICO DE SEGURIDAD Y DEFENSA DE BASES AÉREAS	Defensa de Bases Aéreas	Seguridad Física	TSD	JES
		Operaciones Aéreas Especiales		
		Explosivos		
		Armamento Terrestre y Equipo Especial		
		Seguridad, Custodia y Vigilancia		
		Caninos Militares		
	Inteligencia	Inteligencia Terrestre	TSI	JIN
		Contrainteligencia		
CUERPO LOGÍSTICO AERONÁUTICO	Administración	Administración Logística	LAG	JAL
		Arquitectura e Ingenierías de Apoyo Logístico		
		Periodismo, Producción, Medios de Comunicación y Afines		
		Matemáticas y Ciencias Naturales		
		Administración del Talento Humano		
		Archivistas		
		Músicos		
		Financiera		
	Sanidad	Auxiliar de Enfermería	LAE	DISAN
		Técnico Profesional en Urgencias medicas y/o Atención Prehospitalaria	LUM	
	Telemática	Técnicos en Sistemas	LTE	JAL
		Tecnología en Redes y/o Telecomunicaciones		
		Tecnología en Seguridad de Redes y/o Seguridad Informática	LTS	JIN
	Transportes	Tecnólogo en Mecánica Automotriz	LME	JAL
CUERPO ADMINISTRATIVO	Ciencias de la Salud	Tecnólogo o Técnico Profesional en Regencia de Farmacia	ASRF	DISAN
		Tecnólogo o Técnico Profesional en Farmacia	ASFA	
		Tecnólogo o Técnico Profesional en Imágenes Diagnosticas	ASRD	
		Tecnólogo o Técnico Profesional en Electromedicina	ASEM	
		Tecnólogo o Técnico Profesional en Salud Ocupacional	ASSO	IGEFA
		Tecnólogo o Técnico Profesional Trabajo Social y Comunitario	ASTS	JED
		Tecnólogo o Técnico Profesional en Gestión de Procesos Sociales	ASGP	
	Economía, Administración, Contaduría y Afines	Tecnólogo o Técnico Profesional en Administracion y Afines	AAAD	JAL
		Tecnólogo o Técnico Profesional Auxiliar Contable y Afines	AAAC	
		Tecnólogo o Técnico Profesional en Cine y Fotografía	AACF	
		Tecnólogo o Técnico Profesional en Producción de Radio y Televisión	APRT	
		Tecnólogo o Técnico Profesional en Producción de Cine y/o Televisión	APCT	
		Tecnólogo o Técnico Profesional en Periodismo	AAPE	
		Tecnólogo o Técnico Profesional en Mercadeo y Publicidad	AAMP	
		Tecnólogo o Técnico Profesional en Relaciones Industriales	AARI	

JURDH	
JED	
JEMFA	

212 — 04 ABR. 2012

RESOLUCIÓN NÚMERO ____ DE ____ HOJA Nº

Continuación de la Resolución "Por la cual se adiciona y aclara la Resolución Nº 666 del 12 de octubre de 2011, adoptando unas siglas de especialidades del personal militar de la Fuerza Aérea Colombiana, y se designa la Jefatura o Área funcional para cada Área de Conocimiento"

		Tecnólogo o Técnico Profesional en Secretariado y Afines	AASE	
		Tecnólogo o Técnico Profesional en Comercio Exterior y/o Internacional	AACX	JOL
		Tecnólogo o Técnico Profesional en Administración Hotelería y Turismo	AAHT	JED
	Ingeniería, Arquitectura, Urbanismo y Afines	Tecnólogo o Técnico Profesional en Construcción	AICO	JAL
		Tecnólogo o Técnico Profesional en Electricidad	AIEL	
		Tecnólogo o Técnico Profesional en Electricidad Industrial y Potencia	AIEI	
		Tecnólogo o Técnico Profesional en Sistemas o Afines	AISI	
		Tecnólogo o Técnico Profesional en Telemática	AITL	
		Tecnólogo o Técnico Profesional en Topografía	AITO	
		Tecnólogo o Técnico Profesional Autotrónica	AIAU	
		Tecnólogo o Técnico Profesional Mecánica Automotriz	AIMA	
		Tecnólogo o Técnico Profesional Delineantes de Arquitectura e Ingeniería	AIDE	
		Tecnólogo o Técnico Profesional en Aeromecánica	AIAE	JOL
		Tecnólogo o Técnico Profesional Electromecánica	AIEM	
		Tecnólogo o Técnico Profesional Electrónica	AIET	
		Tecnólogo o Técnico Profesional Industrial	AITI	
		Tecnólogo o Técnico Profesional en Telecomunicaciones	AITC	
	Ciencias Sociales, Derecho y Ciencias Políticas	**Tecnólogo o Técnico Profesional en Criminalística y Ciencias Forenses**	ADCF	JURDH
	Matemáticas y Ciencias Naturales	Tecnólogo o Técnico Profesional Forestal	AMFO	JAL
		Tecnólogo o Técnico Profesional en Estadística y Afines	AMES	
		Tecnólogo o Técnico Profesional en Saneamiento Ambiental	AMSA	

ARTÍCULO 3o. La presente Resolución se actualiza de acuerdo a la organización del servicio público de la educación superior y a las novedades presentadas en las diferentes áreas de conocimiento según el Ministerio de Educación Nacional, la Ley 30 de 1992, demás normas que la modifiquen y adicionen.

ARTÍCULO 4º. La presente Resolución rige a partir de la fecha de su expedición.

Comuníquese y Cúmplase,
Dada en Bogotá D.C., a los 04 ABR. 2012

EL COMANDANTE DE LA FUERZA AÉREA COLOMBIANA,

General TITO SAÚL PINILLA PINILLA

ANEXO C

Malla curricular de la carrera de pregrado Ingeniería informática, impartida en EMAVI.

FUERZAS MILITATRES DE COLOMBIA
FUERZA AEREA COLOMBIANA
ESCUELA MILITAR DE AVIACIÓN "MARCO FIDEL SUAREZ"

PROGRAMA DE INGENIERÍA INFORMÁTICA - PLAN DE ESTUDIOS - 2009

I	II	III	IV	V	VI	VII	VIII	IX	X
272	288	320	320	320	320	320	304	128	144
17 14 3	18 15 3	20 15 5	20 16 4	20 15 5	20 13 7	20 16 4	19 17 2	8 6 2	9 7 2
MATEMATICAS I BGI-I-1101 3 3 0	MATEMATICAS II BGI-I-1202 3 3 0	MATEMATICAS III BGI-I-1303 3 3 0	MATEMATICAS IV BGI-I-1404 3 3 0	MATEMATICAS V BGI-I-1505 3 3 0	INVESTIGACION DE OPERACIONES TE-I-1706 3 2 1	SIMULACION TE-I-1807 3 2 1	SEMINARIO WEB TE-I-2708 2 1 1		
SEMINARIO DE INGENIERIA CP-I-1101 2 2 0	FISICA I BGI-I-1602 3 2 1	FISICA II BGI-I-1703 3 2 1	FISICA III BGI-I-1804 3 2 1	ARQUITECTURA COMPUTACIONAL TE-I-1305 3 2 1	TELEMATICA I TE-I-1906 3 2 1	TELEMATICA II TE-I-2007 3 2 1	TELEMATICA III TE-I-2108 3 2 1	TOPICO ESPECIAL I TE-I-2209 3 2 1	TOPICO ESPECIAL II TE-I-2310 3 2 1
SISTEMAS DE REPRESENTACION COMPUTACIONAL I TE-I-1101 3 2 1	ALGEBRA LINEAL BGI-I-1902 3 3 0	SISTEMAS DE REPRESENTACION COMPUTACIONAL II TE-I-1203 3 2 1	ESTADISTICA Y PROBABILIDAD BGI-I-2004 3 3 0	S.I.G. PARA LA AERONAUTICA I TE-I-1405 3 2 1	S.I.G. PARA LA AERONAUTICA II TE-I-1506 3 2 1	S.I. PARA LA AERONAUTICA TE-I-1607 3 2 1	AUDITORIA DE SISTEMAS GT-I-1608 3 3 0	ENFASIS I CP-I-2409 3 2 1	ENFASIS II CP-I-2510 3 2 1
INFORMATICA I CP-I-1201 3 2 1	INFORMATICA II CP-I-1302 3 2 1	INFORMATICA III CP-I-1403 3 2 1	ANALISIS NUMERICO BGI-I-2104 3 2 1	ANALISIS DE ALGORITMOS CP-I-1905 3 2 1	INGENIERIA DE SOFTWARE I CP-I-2206 3 2 1	INGENIERIA DE SOFTWARE II CP-I-2307 3 2 1	DERECHO AEREO SH-I-1408 3 3 0		INGENIERIA Y MEDIO AMBIENTE BGI-I-2210 3 3 0
LOGICA COMPUTACIONAL CP-I-1501 3 2 1	MATEMATICAS DISCRETAS CP-I-1602 3 2 1	ESTRUCTURAS DE DATOS CP-I-1703 3 2 1	LENGUAJES DE PROGRAMACION CP-I-1804 3 2 1	BASES DE DATOS I CP-I-2005 3 2 1	BASES DE DATOS II CP-I-2106 3 2 1	CONTABILIDAD ADMINISTRATIVA GT-I-1407 3 3 0	ADMINISTRACION INFORMATICA GT-I-1708 3 3 0		
DERECHO CONSTITUCIONAL SH-I-1101 3 3 0	DERECHOS HUMANOS y DIH SH-I-1202 3 3 0	CIENCIA, TECNOLOGIA Y SOCIEDAD SH-I-1303 3 3 0	GEOPOLITICA SH-I-1404 3 3 0	ETICA SH-I-1505 3 3 0	SISTEMAS OPERATIVOS CP-I-2406 3 2 1	PROYECTO DE GRADO I GT-I-1107 2 2 0	PROYECTO DE GRADO II GT-I-1208 2 2 0	PROYECTO DE GRADO III GT-I-1309 2 2 0	
		SEMINARIO DE PROGRAMACIÓN CP-I-2503 2 1 1	SEMINARIO DE INVESTIGACIÓN I GT-I-1904 2 1 1	SEMINARIO S.I.G. TE-I-2605 2 1 1	SEMINARIO DE INVESTIGACIÓN II GT-I-2006 2 1 1	INGENIERIA ECONOMICA GT-I-1507 3 3 0	FORMULACION Y EVALUACION DE PROYECTOS GT-I-1808 3 3 0		

NOMBRE DE LA ASIGNATURA		
CÓDIGO DE LA ASIGNATURA		
TOTAL CRÉDITOS	CRÉDITOS TEORÍA	CRÉDITOS PRÁCTICAS

AREAS GENERALES DEL CONOCIMIENTO PARA INGENIERÍA

FORMACIÓN BÁSICA GENERAL DE INGENIERÍA	FORMACIÓN CIENTÍFICA PROFESIONAL	FORMACIÓN TECNOLOGICA ESPECÍFICA	FORMACIÓN EN GESTIÓN TECNOLOGICA	FORMACIÓN SOCIAL HIUMANÍSTICA

TOTAL HORAS	TOTAL CREDITOS
2736	171

ANEXO D

Contrato entre la FAC y entidades educativas, de los cursos, capacitaciones en temas referentes al ciberespacio.

Curso Ofrecido	Proveedor	Duración
CURSO CYBER INTELLIGENCE PROFESIONAL	McAfee	5 Días
CURSO CYBER INTELLIGENCE INVESTIGATOR	McAfee	5 Días
McAfee Vulnerability Manager (MVM)	McAfee	4 Días
McAfee Web Gateway (MWG)	McAfee	4 Días
McAfee Security Information & Event Management (SIEM)	McAfee	5 Días
McAfee EndPoint Encryption for PC (EEPC)	McAfee	4 Días
McAfee Network Security Platform (NSP)	McAfee	4 Días
CURSO INTRODUCTORIO A LA CRIPTOGRAFIA - CRIPTOANÁLISIS	Cyber Tech	5 Días
CURSO EC-COUNCIL - ADMINISTRACIÓN DE REDES SEGURAS	EC-COUNCIL	5 Días
CURSO EC-COUNCIL - HACKEO ETICO	EC-COUNCIL	5 Días
CURSO EC-COUNCIL - COMPUTACIÓN FORENSE	EC-COUNCIL	5 Días
CURSO EC-COUNCIL - PROGRAMACIÓN SEGURA	EC-COUNCIL	5 Días
CURSO EC-COUNCIL - ANALISTAS DE SEGURIDAD	EC-COUNCIL	5 Días

ANEXO E

Proyecto CEEDEN, Escuela Superior de Guerra, acerca de ciberespacio.

FUERZAS MILITARES DE COLOMBIA
ESCUELA SUPERIOR DE GUERRA

CEESEDEN

PROYECTO DE INVESTIGACIÓN PROFESIONAL

DISEÑO DE LA ESTRATEGIA DE CIBERGUERRA PARA LAS FUERZAS MILITARES DE COLOMBIA

Bogotá D.C.
05 de Abril de 2013

1. INFORMACION GENERAL DEL PROYECTO

Titulo: DISEÑO DE LA ESTRATEGIA DE LA CIBERGUERRA A PARTIR DEL ENFOQUE DE LAS FUERZAS MILITARES DE COLOMBIA										
Investigador Principal: Jairo Andrés Cáceres										
Vinculación a CvLAC:	**SI**		**NO**	**x**	**Código:**					
Correo electrónico: caceresj@esdegue.mil.co										
Teléfono: 3125335806										
Dirección de correspondencia: Carrera 11 No. 102 – 50										
Nombre del Grupo Investigador: Ciberdefensa										
Vinculación a GrupLAC:	**SI** X		**NO**		**Código:**					
Total de investigadores: 3										
Núcleo de Investigación: Naturaleza de la Guerra / Desarrollo Científico y Tecnológico										
Entidad: ESDEGUE (Escuela Superior de Guerra)										
Representante legal: MG. Javier Fernández Leal										
E-mail: fernandezj@esdegue.mil.co										
Cédula de ciudadanía #: 19430629 de Bogotá										
Nit: 830.002.634 - 1						**Dirección:** Carrera 11 No. 102 – 50				
Teléfono: 6204066 EXT 3013						**Fax:**				
Ciudad: Bogotá D.C.						**Departamento:** Cundinamarca				
Tipo de entidades participantes										
Universidad Pública:						**Universidad Privada:**				
Entidad Pública:	X					**Institución Militar:**				X
Centro de Investigación Privado:						**Instituto de Investigación Público:**				
Empresa:	X					**Centro Empresarial o Gremio:**				
CDTs Comunidades:						**ONG**				
Tipo de contribuyente:										
Entidad de derecho público:						**Entidad de economía mixta:**				
Entidad industrial y comercial del estado:						**Entidad de derecho privado:**				
Entidad sin ánimo de lucro:										
Lugar de Ejecución del Proyecto: Escuela Superior de Guerra										
Ciudad: Bogotá						**Departamento:**				
Duración del Proyecto: 12 meses						**Fecha aproximada de inicio:** 10 de marzo				
Tipo de Proyecto: Bibliográfico-Cualitativo										
Investigación Básica:		**Investigación Aplicada:**		X		**Investigación-Acción:**		X		
Tipo de Financiación Solicitada:										
Recuperación		**Cofinanciación:**		X		**Reembolso**				

contingente:				**obligatorio:**	
Valor solicitado:					
Valor contrapartida:					
Valor total del Proyecto:					

TABLA DE CONTENIDO

2. RESUMEN DEL PROYECTO:

"La ciberguerra desde la perspectiva de las Fuerzas Militares de Colombia" es un proyecto de investigación profesional que se ha planteado como misión, construir un enfoque de entendimiento y adecuación de la ciberguerra, y su práctica, inherente a las Fuerzas Militares de Colombia.

Se parte del reconocimiento de que el sector castrense del país debe poseer sus propios fundamentos en esta materia; y no únicamente como ventaja estratégica respecto otras Naciones que aun no se han percatado de la necesidad de comprender el fenómeno y problemáticas, sino también, porque cada actor del sistema internacional posee amenazas y capacidades de respuesta ciberespaciales diferenciales y merece construir su propia fórmula para abordar los nuevos retos a la defensa y seguridad nacional. Más, cuando se parte del principio de, que a diferencia de la disuasión clásica, donde lo que primaba era dar a conocer a los demás el poder militar propio y así lograr periodos de ausencia de conflicto, las capacidades para hacer la guerra en el ciberespacio se mantienen en el más alto secreto de Estado.

En esta medida, el proyecto de investigación se ha diseñado para cumplir un objetivo muy claro y favorable para la labor constitucional del sector defensa: *la construcción de un enfoque de entendimiento y adecuación de la ciberguerra inherente al Estado y Fuerzas Militares de Colombia*.

Para dar cumplimiento a la misión propuesta, se ha formulado una operación sustentada en el cumplimiento de tres objetivos específicos: 1) construir un inventario de conceptos y términos acerca de la ciberguerra inherentes al escenario colombiano y sus Fuerzas Militares; 2) originar un estado del arte sobre la relación del Estado colombiano y sus Fuerzas de defensa con la ciberguerra y sus diversos componentes y categorías; y 3) elaborar la visón estratégica de la ciberguerra en las FF.MM. de Colombia.

DESCRIPTORES / PALABRAS CLAVE:

Ciberguerra, ciberespacio, Internet, ciberdefensa, ciberterrorismo, ciberataque, computadores, Fuerzas Militares, defensa y seguridad nacional.

3. DEFINICIÓN DEL PROBLEMA

3.1. DESCRIPCIÓN DEL PROBLEMA

La ciberguerra, es en el presente un tema insustituible al interior de las agendas gubernamentales y los Organismos de la defensa y seguridad Nacional. El Ejecutivo, los niveles decisores de política pública, las Fuerzas Militares, Cuerpos de inteligencia y policiacos han asimilado que su labor ahora también se ha trasladado a la *World Wide Web*, y que por ende, las iniciativas relacionadas con el capital humano, tecnológico, legislativo y jurídico no deben ser paulatinas sino inmediatas.

Desde diversos flancos se pude dilucidar la necesidad de códigos de conducta para la guerra y defensa del ciberespacio. Es innegable que la información se ha convertido en un bien inmaterial que soporta gran cantidad de las actividades humanas; información secreta del estado, comunicados e inteligencia militar, estrategias de las industrias y empresas nacionales, y no menos importante, la información de la ciudadanía.

No en vano, el sistema internacional ya ha sido testigo de cómo la República Popular de China, por medio de la división de ciberguerra de su Ejército Popular de Liberación, desde el 2002 viene ciberatacando servidores de información gubernamental y privada de los países industrializados con el fin de saquear su información de alto valor. En esta misma línea, nada desacertado estuvo Allen Speller, del SANS Institute, cuando en el año 2008 estableció de manera más concreta que la integración de los sistemas y redes informáticas de compañías como Raytheon, Lockheed Martin, Boeing o Northrup Grumman a la Internet, pondría en grave riesgo la tecnología de defensa y seguridad de los EE.UU.[1] Cuatro años después, y después de haber *hackeado* los sistemas del

[1] BRENER, Susan W. Cyberthreats: the emerging fault lines of the Nation State. OXFORD University Press. New York, 2009

Pentágono y Lockheed Martin, el principal contratista aeroespacial del sector defensa estadounidense, los chinos lograron reproducir su propio prototipo de F-22 Raptor; el J-20.

Pese a la gravead que por sí mismo ya puede significar este escenario, la amenaza no se ha contenido allí; o en otras palabras, el ciberespionaje no es la única táctica que el ser humano ha aprendido a ejecutar mediante las tecnologías de la información y la comunicación.

Es innegable, que la globalización al demandar procesos innovadores que se articularan con nuevos parámetros tiempo-espaciales para la comunicación y transferencia de datos y conocimiento, llevó al Estado Nación y los actores del sistema internacional a traspalar sus actividades, funcionamiento y supervivencia sobre la lógica de la comunicación en red, virtual y en tiempo real/global.

Cuando se analiza la sinergia y alta dependencia que las mismas sociedades han constituido en torno a las tecnologías de la Información y la Comunicación, se es presente de la concatenación de un concepto/realidad más trascendente que la misma Internet; el ciberespacio. En la instancia en que los computadores y los sistemas de comunicación en red globales se habilitaron como soportes eficientes y eficaces para los procesos humanos, se modelaron realidades intrincadas de comprender y sobrellevar desde la óptica de la defensa del Estado Nación.

Al haber integrado la infraestructura crítica de los Estados al ciberespacio se produjo un fenómeno de virtulización de los "centros de gravedad", atendiendo a este concepto como lo hizo en su momento Clausewitz, o Warden desde su teoría de los "cinco anillos".

En tanto la informática se convirtió en tecnología cibernética para controlar el entorno, reactores nucleares, hidroeléctricas, controladores de tráfico (aéreo, terrestre y marítimo), bolsas de valores, sistemas bancarios, satélites, sistemas de defensa, armamento (vehículos no tripulados) y las redes de comunicación, entre otros ejemplos, se abrió la posibilidad de que algún sujeto o agrupación, con el suficiente conocimiento en códigos a

base de binarios para crear armas digitales, pusiera estos elementos a sus disposición; bien fuera por fines políticos, terroristas, lucrativos o contestatarios.

En 2007 Estonia, y posteriormente en 2008 Georgia fueron atacados cibernéticamente por Rusia a nivel bancario, gubernamental, transacciones *on-line*, comunicaciones y medios de información. Paralelamente, durante este último año, mientras se ejecutaba la Operación israelí Plomo Fundido en la Franja de Gaza, bandas de hacker pro-palestinos atacaron la red informática gubernamental y de defensa de Israel. En 2010 el reactor nuclear iraní de Busher, y base de las centrifugadoras de uranio del programa, fue deshabilitado antes de su inauguración por una ciberarma denominada como *stuxnet*.

Lo más desconcertante en materia de ciberguerra acaecido hasta hoy, ha sido la usurpación de un avión no tripulado de espionaje (UAV) estadounidense por parte del gobierno iraní, cuando *soldados de la información* de este Estado *hackearon* el sistema de control de la nave para dirigirla a aterrizar a una base militar nacional; rompiendo así con la lógica de emplear las defensas antiaéreas, y pasar a la posibilidad de hacer procesos de tecnología inversa sobre el material del contrario.

Claramente, los países desarrollados debido a su alta dependencia a las tecnologías informáticas, han iniciado el camino de la ciberguerra y ciberdefensa años atrás. No obstante, en la actualidad son escasos los países que poco tiene que ver con el ciberespacio.

Colombia es un caso concreto. Si bien es un Estado que se encuentra en desarrollo, no se excluye que gran parte del funcionamiento del sector gubernamental, de los sistemas militares, o bien, que parte de la infraestructura crítica colombiana se apoya en tecnologías informáticas y sistemas de información que se han integrado al ciberespacio.

3.2. FORMULACIÓN DEL PROBLEMA

¿Cuál es el enfoque de entendimiento y adecuación de la ciberguerra más apropiado para adoptarse como característico de las Fuerzas Militares de Colombia?

3.3. ANTECEDENTES DEL PROBLEMA

La construcción y evolución del ciberespacio, en compañía de las potencialidades comunicacionales e informáticas ofrecidas por las TIC, se ha constituido como un fenómeno de transformación significativo en el ámbito de la seguridad y defensa nacional.

En la actualidad, no es un secreto en el mundo que diversos Gobiernos y gran parte de los actores armados ilegales (que bien libran conflictos terroristas o subversivos, o que buscan objetivos netamente lucrativos), así como individuos y grupos societales activistas han visualizado en los computadores y las redes informáticas poderosos mecanismos para detentar o minar el orden y soberanía de un Estado Nación. No en vano, en el plano de las conflagraciones bélicas los conceptos de ciberguerra, ciberterrorismo y cibercrimen, y problemáticas de orden social como el ciberactivismo se han configurado como amenazas preponderantes en el presente.

En correlación, ya diversos Estados en el sistema internacional han comenzado a estructurar sus políticas y modelos de conservación nacional con base en las capacidades y alcances de las amenazas cibernéticas que cada uno padece. Desde otra perspectiva, han iniciado su propio curso de construcción de las capacidades de ciberguerra para defender sus intereses nacionales, estratégicos y humanos.

Parte fundamental de este curso de acción se ha traducido en la construcción de una visión propia que le permita a cada actor modelar sus estrategias en ciberguerra conforme sus características y necesidades innatas. Así, las operaciones en ésta nueva categoría de la guerra, tanto desde su doctrina de operaciones especiales, así como desde su carácter defensivo se acompañan de una comprensión académica teórica, conceptual y práctica del objeto de estudio como producto de su investigación profesional.

Colombia, a través de su política de ciberdefensa y la conformación de su Comando Conjunto Cibernético de las FF.MM. ya comenzó su carrera en ciberguerra y ciberdefensa, no obstante en materia de desarrollo de investigación profesional o científica para comprender el nuevo ambiente de combate se encuentra tardío.

4. JUSTIFICACIÓN

Las Fuerzas Militares como garantes de la defensa del Estado Nación colombiano, deben contar con un marco de comprensión integral acerca de la transformación del ciberespacio en una dimensión en donde las amenazas provenientes de otros Estados y actores asimétricos se potencian con éxito y pueden llegar a presentan efectos devastadores.

En este sentido, este proyecto de investigación se configura como efectivo marco de generación de conocimiento en esta materia. En primera instancia, porque le permitirá al sector castrense del país asimilar, desde una perspectiva integral, el nuevo teatro de la guerra al que se ha hecho ya mención. Segundo, porque permitirá al Estado y sus FF.MM. obtener un "autoconocimiento" tanto de sus capacidades así como de sus vulnerabilidades frente a la ciberguerra.

Finalmente, y como producto estratégico del proyecto, se ofrecerá al sector defensa una visión estratégica de la ciberguerra, a través de una serie de documentos que podrán servir de consulta para el accionar militar en el ciberespacio; y en los cuales un enfoque inherente a la realidad y requerimientos de Colombia será el elemento transversal.

5. OBJETIVOS

5.1. OBJETIVO GENERAL

Originar un enfoque de entendimiento y adecuación de la ciberguerra inherente al Estado y Fuerzas Militares de Colombia.

5.2. OBJETIVOS ESPECÍFICOS

- Construir los conceptos de ciberguerra propios de las FF.MM. de Colombia.

- Desarrollar un estado del arte sobre la relación del Estado colombiano y sus Fuerzas de defensa con la ciberguerra, sus amenazas y su ejercicio.

- Constituir el marco de visión estratégica de la ciberguerra de las Fuerzas Militares de Colombia.

6. DISEÑO METODOLÓGICO

Para el óptimo desarrollo de esta iniciativa, se ha asumido una estrategia consistente en una investigación de tipo mixta mediante la sinergia de la **Investigación Bibliográfica** y la **Investigación Cualitativa.**

Investigación Bibliográfica, ya que es de suma importancia porque ofrece el enfoque de investigación del estado del arte; el cual se requiere para el procedimiento de análisis profundo en donde se presenta una ficha de recolección de información y pretende hacer un seguimiento del proceso de investigación de una temática determinada durante un tiempo predefinido, ya sea con tesis, artículos o documentos de diverso índole.

Simultáneamente, la Investigación Cualitativa proporcionará el enfoque del estudio de caso que sistemáticamente explora y observa un solo individuo o individuos únicos y busca reconstruir el período objetivamente con base en información y conocimiento confiable.

Como lo establecen Bonilla y Rodríguez:

> "Las investigaciones de tipo cualitativo se caracterizan porque la interpretación de sus datos consiste en un proceso dinámico que se nutre de todo el trabajo de inducción analítica iniciado desde el momento mismo de la recolección.

> Interpretar es buscar sentido y encontrar significado a los resultados, explicando las tendencias descriptivas y buscando relaciones entre las diferentes dimensiones que permitan construir una visión integral del problema"[2]

6.1. TIPO DE INVESTIGACIÓN

La presente investigación es de tipo mixta. Esto, gracias a que se fundamenta en primera medida en una **Investigación Bibliográfica** para desarrollo de estado del arte. Y simultáneamente, porque empleara el enfoque del estudio de caso de la **Investigación Cualitativa**.

6.2. UNIDAD DE ANÁLISIS

La unidad de análisis se definió a partir de los dos líneas de información y conocimiento en materia en materia de ciberguerra a partir del Estado colombiano y sus FF.MM.: 1) comprender la ciberguerra como fenómeno y práctica desde una perspectiva holística; y 2) obtener una radiografía del nivel de relación de Colombia y sus Fuerzas Militares con la ciberguerra.

Primero, con relación a comprender la ciberguerra como fenómeno y práctica desde una perspectiva holística, se diseño la unidad de análisis para concentrarse en las teorías, desarrollo conceptual y estudio casuístico del fenómeno de la ciberguerra; las formas de ciberataques que se han registrado hasta el momento para comprender el nivel táctico de esta guerra; también, como otros Estados Nación están asumiendo los riesgos de la ciberguerra, así como sus estrategias para la concatenación de poder nacional y militar en ciberguerra; y finalmente, por medio del estudio de la aplicación de los marcos jurídicos internacionales sobre la ciberguerra como práctica contemporánea.

---

[2] BONILLA, Castro Elsy y RODRÍGUEZ, Sehk Penélope. *Más allá del dilema de los métodos*. Grupo Editorial Norma, Bogotá; 1997.

Segundo, conforme con el panorama del nivel de relación de Colombia y sus Fuerzas Militares con la ciberguerra, el tema se delimitó para observar: el grado de dependencia que la infraestructura crítica y sistemas de comunicación de Colombia mantienen en el presente frente al ciberespacio; las agresiones que ha sufrido el Estado a su infraestructura informática; el nivel de sinergia de las FF.MM, con las TIC y el ciberespacio, así como las capacidades adquiridas para cumplir con su labor constitucional en el ciberespacio; y en última medida, la legislación que exista hoy en día en el país para determinar comprensión y formas de actuación de la ciberguerra.

6.3. UNIDAD DE TRABAJO

La unidad de trabajó se configura con base en investigaciones, documentos de trabajo, libros, publicaciones gubernamentales, conceptos militares, entrevistas a autoridades en la materia (académicas y militares), y visitas a instalaciones destinadas a cumplir un rol en materia de ciberguerra en el país.

6.4. INSTRUMENTOS PARA LA RECOLECCIÓN DE INFORMACIÓN

- Revisión de fuentes
- Entrevistas
- Visitas de Campo

6.5. ANÁLISIS DE INFORMACIÓN

Consiste en describir y justificar el proceso que se va a utilizar para clasificar, registrar y codificar la información recolectada. Además debe tener claridad de la técnica analítica que va a utilizar para responder a las preguntas de investigación formuladas y obtener las conclusiones respectivas.

6.6. PROCEDIMIENTO

Objetivo Específico	Fase metodológica	Actividades
Construir los conceptos de ciberguerra propios de las FF.MM. de Colombia.	1	-Desarrollar un estado del arte y estado de la cuestión sobre la ciberguerra. -Comprender las diversas formas de emplear la ciberguerra como forma de ataque. -Analizar el tratamiento de la ciberguerra en otros actores del sistema internacional. -Explorar la práctica e implicaciones de la ciberguerra a la luz del derecho Internacional.
Desarrollar un estado del arte sobre la relación del Estado colombiano y sus Fuerzas de defensa con la ciberguerra, sus amenazas y su ejercicio.	2	-Realizar un análisis acerca del nivel de dependencia del Estado Colombiano al ciberespacio desde la perspectiva de la vulnerabilidad. -Construir un estado del arte acerca de las agresiones cibernéticas que han impactado al Estado colombiano. -Desarrollar un estado de la cuestión acerca de la sinergia de las FF.MM. de Colombia a las TIC, y sus capacidades para adaptarse a la ciberguerra. -Explorar la práctica e implicaciones de la ciberguerra a la luz del derecho colombiano.
Constituir el marco de visión estratégica de la ciberguerra de las Fuerzas Militares de Colombia	3	-Producir la primera *Apreciación Político Estratégica Nacional (APEN) del ciberespacio.* -Constituir una propuesta de *Manual de Doctrina Operativo*

		para la Ciberguerra. -Establecer un documento propuesta para la *aplicación y sustentación del empleo de la ciberguerra desde el marco del derecho.*

7. CONFORMACIÓN Y TRAYECTORIA DEL GRUPO DE INVESTIGACIÓN

NOMBRE	ESCOLARIDAD	EXPERIENCIA	DATOS ADICIONALES	TRABAJOS DESARROLLADOS RELACIONADOS CON EL TEMA	PUBLICACIONES RELACIONADAS CON EL TEMA
Observatorio Militar en Ciberguerra (OMEC)	(a espera de su aprobación y conformación)	(a espera de su aprobación y conformación)	(a espera de su aprobación y conformación)	1 (de ser aprobado y conformado)	0

ANEXO 1. Formato Hoja de vida Investigadores, Asesores.

HOJA DE VIDA (RESUMEN)		
IDENTIFICACIÓN DEL INVESTIGADOR PRINCIPAL / COINVESTIGADOR / ASESOR:		
Apellidos: SANCHEZ LOZANO	Nombre: MARTHA LILIANA	
Fecha de Nacimiento 13 de nov 1970	Nacionalidad: Colombiana	
Correo electrónico: sanchezm@esdegue.mil.co		
Documento de identidad: 39756252	Tel/fax 620 40 66 Ext. 20604	
Entidad donde labora ESDEGUE	Tel/fax 620 40 66 Ext. 20604	
Cargo o posición actual Jefe de Telemática-		
TÍTULOS ACADÉMICOS OBTENIDOS		
ÁREA/DISCIPLINA	UNIVERSIDAD	AÑO
MBA- Administración	Universidad de los Andes	2011
Especialista en Sistemas de Información	Universidad de los Andes	2007
Oficial FAC	Escuela Militar de Aviación	1993
Ingeniera de Sistemas	Universidad Católica de Colombia	1986
CAMPOS DE LA CIENCIA Y LA TECNOLOGÍA EN LOS CUALES ES EXPERTO		
Administración, Desarrollo tecnológico e innovación		

CARGOS DESEMPEÑADOS EN LOS ÚLTIMOS 5 AÑOS				
INSTITUCIÓN	CARGO	D	M	A
ESDEGUE	Jefe de Telemática	20	01	2012
COFAC	Jefe de Planeación Logística	10	01	2007
PUBLICACIONES RECIENTES				
PATENTES, PROTOTIPOS U OTRO TIPO DE PRODUCTOS TECNOLÓGICOS O DE INVESTIGACIÓN OBTENIDOS EN LOS ÚLTIMOS 5 AÑOS				
Prototipo de simulación de toma de decisiones para administración y piorizaciónn de los recursos de inversión FAC – Tesis unidades nota- 5.0				

HOJA DE VIDA (RESUMEN)		
IDENTIFICACIÓN DEL INVESTIGADOR PRINCIPAL / COINVESTIGADOR / ASESOR:		
Apellidos: CÁCERES GARCÍA	Nombre: JAIRO ANDRÉS	
Fecha de Nacimiento 20 NOV 60	Nacionalidad:COLOMBIANO	
Correo electrónico: CACERESJ@ESDEGUE.MIL.CO		
Documento de identidad: 19´390.097	Tel/fax 3125335806	
Entidad donde labora ESDEGUE	Tel/fax 6206524	
Cargo o posición actual DOCENTE		
TÍTULOS ACADÉMICOS OBTENIDOS		
ÁREA/DISCIPLINA	UNIVERSIDAD	AÑO
ESPECIALISTA EN INFORMATICA	AUTONOMA DE GUADALAJARA MEJICO	1980
ESPECIALIZACIÓN EN GERENCIA RRHH	SERGIO ARBOLEDA	2000
MAESTRIA EN INGENIERIA LOGISTICA	ACADEMIA POLITEC EJERCITO CHILE Y PONTIFICIA UNIV CATÓLICA DE VALPARAISO	2007
ADMINISTRADOR LOGÍSTICO	ESCUELA DE LOGÍSTICA EJC NAL	2004
CAMPOS DE LA CIENCIA Y LA TECNOLOGÍA EN LOS CUALES ES EXPERTO		

CARGOS DESEMPEÑADOS EN LOS ÚLTIMOS 5 AÑOS				
INSTITUCIÓN	CARGO	D	M	A
ESCUELA DE GUERRA FFMM	DOCENTE INVESTIGADOR	2	3	11
EMPRESAS PRIVADAS	CONSULTOR Y CONFERENCIENTE	3	2	9

PUBLICACIONES RECIENTES				
(Por lo menos las cinco publicaciones más importantes que haya hecho en los últimos cin				
PATENTES, PROTOTIPOS U OTRO TIPO DE PRODUCTOS TECNOLÓGICOS O DE INVESTIGACIÓN OBTENIDOS EN LOS ÚLTIMOS 5 AÑOS				

HOJA DE VIDA (RESUMEN)

IDENTIFICACIÓN DEL INVESTIGADOR PRINCIPAL / COINVESTIGADOR / ASESOR:	
Apellidos: Gaitán Rodríguez	Nombre: Andrés
Fecha de Nacimiento 22 de abril 1982	Nacionalidad: colombiano
Correo electrónico: andresgaro@gmail.com	
Documento de identidad: 80184687	Tel/fax: 3173005770
Entidad donde labora: Esdegue	
Cargo o posición actual: Director de núcleo	

TÍTULOS ACADÉMICOS OBTENIDOS		
ÁREA/DISCIPLINA	UNIVERSIDAD	AÑO
Ciencia política	Universidad Javeriana	2007
Seguridad y defensa	Escuela Superior de Guerra	2011

CAMPOS DE LA CIENCIA Y LA TECNOLOGÍA EN LOS CUALES ES EXPERTO

Seguridad y defensa
Ciberguerra, TICS, ciberdefensa.

CARGOS DESEMPEÑADOS EN LOS ÚLTIMOS 5 AÑOS				
INSTITUCIÓN	CARGO	D	M	A
Escuela Superior de Guerra	Director de núcleo			2010-
Contraloría de Cundinamarca	Asesor			2008-2010

PUBLICACIONES RECIENTES

(Por lo menos las cinco publicaciones más importantes que haya hecho en los últimos cinco años).

PATENTES, PROTOTIPOS U OTRO TIPO DE PRODUCTOS TECNOLÓGICOS O DE INVESTIGACIÓN OBTENIDOS EN LOS ÚLTIMOS 5 AÑOS

No.

8. RESULTADOS/PRODUCTOS ESPERADOS Y POTENCIALES BENEFICIARIOS:

Resultado/Producto esperado	Indicador	Beneficiario

Cartilla de los conceptos de ciberguerra inherentes al Estado Colombiano.	Cartilla	Sector defensa, comunidad académica militar y civil del país.
Actividad académica de divulgación y socialización de resultados.	Mesa de trabajo, conferencia, conversatorio, seminario	Sector defensa, comunidad académica militar y civil del país.
Artículo para publicación sobre el estado del arte de sinergia del Estado colombiano con el ciberespacio	Artículo de investigación	Sector defensa, comunidad académica militar
Actividad académica de divulgación y socialización de resultados.	Mesa de trabajo, conferencia, conversatorio, seminario	Sector defensa, comunidad académica militar
Apreciación Político Estratégica Nacional (APEN) del ciberespacio.	Documento APEN	Gobierno Nacional y Sector Defensa
Manual de Doctrina Operativo para la Ciberguerra.	Manual	Sector Defensa
Cartilla de aplicación y sustentación del empleo de la ciberguerra desde el marco del derecho.	Cartilla	Sector Defensa
Actividad académica de divulgación y socialización de resultados.	Mesa de trabajo, conferencia, conversatorio, seminario	Gobierno Nacional y Sector Defensa

9. IMPACTOS ESPERADOS A PARTIR DEL USO DE LOS RESULTADOS

Impacto esperado	Plazo: corto (1-4 años), mediano (5-9 años), largo (10 años o más)	Indicador verificadores	Supuestos*

10.CRONOGRAMA

* Los supuestos indican los acontecimientos, las condiciones o las decisiones, necesarios para que se logre el impacto esperado.

FASES Y ACTIVIDADES	MES
FASE 0 – PLANEACION DEL PROYECTO	**Semana 25-31 de marzo a la semana 1-5 de abril**
Tema de investigación	
Idea de investigación	
Elección de línea de investigación	
Justificación de la investigación	
Descripción del problema	
Formulación del problema	
Selección de variables	
Formulación de objetivos, hipótesis , tipo de investigación, diseño y operacionalización de variables	
Selección de métodos de recolección de información	
FASE 2 - CONSTRUIR LOS CONCEPTOS DE CIBERGUERRA PROPIOS DE LAS FF.MM. DE COLOMBIA.	**Semana 8-14 de abril a la semana 24-30 de junio**
-Desarrollar un estado del arte y estado de la cuestión sobre la ciberguerra.	
-Comprender las diversas formas de emplear la ciberguerra como forma de ataque.	
-Analizar el tratamiento de la ciberguerra en otros actores del sistema internacional.	
-Explorar la práctica e implicaciones de la ciberguerra a la luz del derecho Internacional.	
FASE 3 **DESARROLLAR UN ESTADO DEL ARTE SOBRE LA RELACIÓN DEL ESTADO COLOMBIANO Y SUS FUERZAS DE DEFENSA CON LA CIBERGUERRA, SUS AMENAZAS Y SU EJERCICIO.**	**Semana 1-7 de julio a la semana 9-15 de septiembre**
-Realizar un análisis acerca del nivel de dependencia del Estado Colombiano al ciberespacio desde la perspectiva de la vulnerabilidad.	
-Construir un estado del arte acerca de las agresiones cibernéticas que han impactado al Estado colombiano.	
-Desarrollar un estado de la cuestión acerca de la sinergia de las FF.MM. de Colombia a las TIC, y sus capacidades para adaptarse a la ciberguerra.	
-Explorar la práctica e implicaciones de la ciberguerra a la luz del derecho colombiano	
FASE 4 CONSTITUIR EL MARCO DE VISIÓN ESTRATÉGICA DE LA CIBERGUERRA DE LAS FUERZAS MILITARES DE COLOMBIA	**Semana 16-22 de septiembre a la semana 25-30 de noviembre.**
-Producir la primera *Apreciación Político Estratégica Nacional (APEN) del ciberespacio.*	
-Constituir una propuesta de *Manual de Doctrina Operativo para la Ciberguerra.*	
-Establecer un documento propuesta para la *aplicación y sustentación del empleo de la ciberguerra desde*	