El manejo de la ciberseguridad en Fuerzas Armadas

Guerrero Villafuerte, Renzo Oswaldo y Proaño Andrade, Carlos Patricio

Vicerrectorado de Investigación, Innovación y Transferencia de Tecnología

Centro de Posgrados

Maestría en Estrategia Militar Terrestre

Trabajo de titulación, previo a la obtención del título de Magíster en Estrategia Militar Terrestre

TCRN. E.M. Bravo Terán, Germán Vinicio

24 de julio de 2020

URKUND

Urkund AnalysisResult

Analysed Document:	EL MANEJO DE LA CIBERSEGURIDAD EN FUERZAS ARMADAS
aprobado.pdf (D77521555) Submitted:	8/6/2020 3:32:00 AM
Submitted By:	eegalarza@espe.edu.ec
Significance:	8 %

Sources included in the report:

Trabajo de titulación completa.....

https://es.....

http://www....

https://www...

https://www...

Instances where selected sources appear:

Certificó que el trabajo de titulación, "El manejo de la Ciberseguridad en Fuerzas Armadas", fue realizado por los señores TCRN. DE E.M Guerrero Villafuerte Renzo Oswaldo y TCRN. DE E.M Proaño Andrade Carlos Patricio, el mismo que ha sido revisado en su totalidad, analizado por la herramienta de verificación de similitud de contenido; por lo tanto, cumple con los requisitos teóricos, científicos, técnicos, metodológicos y legales establecidos por la Universidad de Fuerzas Armadas ESPE, razón por la cual me permito acreditar y autorizar para que lo sustente públicamente.

Firma:

TCRN. E.M Bravo Terán, Germán Vinicio

Director

C.C: **0501483598**

VICERRECTORADO DE INVESTIGACIÓN, INNOVACIÓN Y TRANSFERENCIA DE TECNOLOGÍA

CENTRO DE POSGRADOS

CERTIFICACIÓN

Certifico que el trabajo de titulación, **"El Manejo de la ciberseguridad en Fuerzas Armadas"** fue realizado por los señores **Tcrn De E.M Guerrero Villafuerte Renzo Oswaldo, y Tcrn De E.M Proaño Andrade Carlos Patricio,** el mismo que ha sido revisado y analizado en su totalidad, por la herramienta de verificación de similitud de contenido; por lo tanto, cumple con los requisitos legales, teóricos, científicos, técnicos y metodológicos establecidos por la Universidad de las Fuerzas Armadas ESPE, razón por la cual me permito acreditar y autorizar para que lo sustente públicamente.

Sangolquí, 24 de julio de 2020

Firma:

TCRN. E.M Bravo Terán, Germán Vinicio

Director

C.C: **0501483598**

VICERRECTORADO DE INVESTIGACIÓN, INNOVACIÓN Y TRANSFERENCIA DE TECNOLOGÍA

CENTRO DE POSGRADOS

RESPONSABILIDAD DE AUTORÍA

Nosotros, **Tcrn De E.M Guerrero Villafuerte Renzo Oswaldo,** con cédula de ciudadanía N° **171113899-6 y Tcrn De E.M Proaño Andrade Carlos Patricio,** con cédula de ciudadanía **N° 100174326-7**, declaramos que el contenido, ideas y criterios del trabajo de titulación*:* **"El manejo de la ciberseguridad en Fuerzas Armadas"**, es de nuestra autoría y responsabilidad, cumpliendo con los requisitos legales, teóricos, científicos, técnicos y metodológicos establecidos por la Universidad de las Fuerzas Armadas ESPE, respetando los derechos intelectuales de terceros y referenciando las citas bibliográficas.

Sangolquí, 24 de julio de 2020

Firma (s)

Guerrero Villafuerte Renzo O.
C.C.: 171113899-6

Firma (s)

Proaño Andrade Carlos Patricio
C.C.:100174326-7

VICERRECTORADO DE INVESTIGACIÓN, INNOVACIÓN Y TRANSFERENCIA DE TECNOLOGÍA

CENTRO DE POSGRADOS

AUTORIZACIÓN DE PUBLICACIÓN

Nosotros, **Tcrn De E.M Guerrero Villafuerte Renzo Oswaldo,** con cédula de ciudadanía **N° 171113899-6 y Tcrn De E.M Proaño Andrade Carlos Patricio,** con cédula de ciudadanía **N° 100174326-7,** autorizamos a la Universidad de las Fuerzas Armadas ESPE publicar el trabajo de titulación: **"El manejo de la ciberseguridad en Fuerzas Armadas",** en el Repositorio Institucional, cuyo contenido, ideas y criterios son de nuestra responsabilidad.

Sangolquí, 24 de julio de 2020

Firma (s)

Guerrero Villafuerte Renzo O.
C.C.: 171113899-6

Firma (s)

Proaño Andrade Carlos Patricio,
C.C.:100174326-7

Dedicatoria

El presente trabajo, realizado con esfuerzo y perseverancia a las siguientes personas que ocupan un lugar muy especial en mi Corazón a:

Dios, por ser siempre el que guía permanentemente mis pasos

Mis Padres: **Raúl y Florita**, por ser ese ejemplo de trabajo y honestidad e inspiración para mi superación profesional.

Mi Esposa: Gabriela por todo su apoyo y amor en cada momento.

Mi amado Hijo Carlos Daniel, un ser extraordinario quien ve en mi un ejemplo a seguir, a mi pequeño Emilio Sebastián, motive de inspiración en mi vida, gracias por su sincera y absoluta entrega, que me guía y fortalece cada día.

Mis hermanos: Jandyr Raúl y Cristian, quien con su ejemplo y cariño han sabido en caminarme dentro de la noble Carrera de las armas, quienes depositaron fe en mis capacidades y solidaridad, me motivaron a seguir Adelante.

Carlos Patricio Proaño Andrade

Agradecimiento

La presente tesis se la dedico a mi familia que gracias a su apoyo pude concluir con éxito.

A mis Padres y hermanos por su apoyo y confianza en todo lo necesario para cumplir mis objetivos como un militar hecho y derecho.

A la Universidad de Las Fuerzas Armadas, por haberme brindado la oportunidad de acrecentar mis conocimientos.

Al Glorioso Ejército Ecuatoriano por contribuir el desarrollo profesional de sus soldados.

Guerrero Villafuerte Renzo O

INDICE DE CONTENIDOS

Capítulo I **17**

El problema. **17**

Planteamiento del Problema. 17

Formulación del Problema. 20

Preguntas de Investigación. 20

Objeto de Estudio. 21

Campo de Acción. 25

Delimitación de la Investigación 26

Delimitación Temática. 26

Delimitación Espacial. 26

Delimitación Temporal. 27

Justificación de la Investigación. 27

Originalidad 27

Relevancia 27

Interés 28

Factibilidad 29

Objetivos de la Investigación. 29

Objetivo General. 29

Objetivos Específicos 30

Capítulo II **31**

MARCO TEÓRICO. **31**

Antecedentes de la Investigación. 31

Fundamentación teórica. 34

Fundamentación General 37

Fundamentación Específica 37

Base Legal 41

Hipótesis 43

Sistema de Variables 43

Variables Independientes. 43

Variables dependientes. 44

Conceptualización y Operacionalización de las variables 45

Conceptualización y Operacionalización de las variables independientes. 45

Conceptualización y Operacionalización de las variables dependientes. 48

Capítulo III 49

MARCO METODOLÓGICO. 49

Enfoque de la Investigación. 49

Tipo de Investigación. 56

Población. 57

Muestra. 58

Métodos de Investigación. 59

Técnicas de Recolección de datos. 59

Instrumentos de Recolección de datos. 59

Técnicas para el análisis e interpretación de Datos. 61

Análisis De Resultados De La Entrevista Y Encuesta. 61

Aplicación de la entrevista 61

Entrevista 62

Análisis de la entrevista 67

Tabulación de datos de las encuestas. 68

Capítulo IV 78

DESARROLLO DE LOS OBJETIVOS. 78

Primer Objetivo Específico y/o Tarea Científica 78

Introducción 78

Conocimiento del Hecho 78

Análisis 80

Conclusiones Parciales 82

Segundo Objetivo Específico y/o Tarea Científica 83

Introducción 83

Conocimiento del Hecho 84

Análisis 85

Conclusiones Parciales 87

Tercer Objetivo Específico y/o Tarea Científica 88

Introducción 88

Conocimiento del Hecho 89

Análisis 90

Conclusiones Parciales 91

Cuarto Objetivo Específico y/o Tarea Científica 92

Introducción 92

Conocimiento del Hecho 94

Análisis 95

Conclusiones Parciales 97

Capítulo V 99

Propuesta. 99

Título de la propuesta 99

Objetivo de la propuesta. 99

Alcance de la propuesta. 100

Desarrollo de la propuesta 104

Introducción 104

Conocimiento del Hecho 105

Análisis 107

Conclusiones Parciales 122

Introducción 123

Conocimiento del Hecho 125

Análisis 126

Conclusiones Parciales 149

Introducción 150

Conocimiento del Hecho 151

Análisis 153

Conclusiones Parciales 155

Introducción 156

Conocimiento del Hecho 157

Análisis 159

Conclusiones Parciales 177

Fundamentación. Doctrinaria, Técnica, Documental, Filosófica 180

Fundamentación. Histórica, Social, Cultural, etc 183

Validación de la propuesta 186

Conceptualización de la propuesta. 188

Método y criterios de Validación. 191

Validación. 198

Matriz de Cuadrícula. 198

Capítulo VI 200

CONCLUSIONES Y RECOMENDACIONES 200

Conclusiones 200

Propuesta 202

Recomendaciones 205

BIBLIOGRAFÍA 211

ANEXOS 214

INDICE DE TABLAS

Tabla 1 Tabulación de respuestas a encuestas en www.docs.google.com/forms _ 77

Tabla 2 Conformación del Sistema de Ciberdefensa, según Acuerdo Ministerial 281, Art 1, del 24 de septiembre *de 2014* _ 140

Tabla 3 Propuesta de matriz general inicial de capacidad operativa del COCIBER _____ 204

INDICE DE FIGURAS

Figura 1 Porcentaje de la misión que cumple el COCIBER _69

Figura 2 Porcentaje de las capacidades del COCIBER _ 70

Figura 3 Porcentajes de las amenazas y riesgos de la Ciberdefensa _ 71

Figura 4 Porcentaje de la capacidad operativa del comando de Ciberdefensa _ *72*

Figura 5 Porcentaje de la capacidad operativa del comando de Ciberdefensa _ 73

Figura 6 Porcentaje de componentes adicionales en matriz de capacidad operativa del Comando de Ciberdefensa _ 74

Figura 7 Porcentajes de proyectos a fortalecer el Comando de Ciberdefensa _ 75

Figura 8 Porcentajes de proyectos a fortalecer el Comando de Ciberdefensa _ 76

Resumen

La Ciberdefensa, ha adquirido gran relevancia mundial en las últimas décadas. El Ministerio de Defensa Nacional, estableció en la Agenda Política de la Defensa Nacional, la necesidad de la protección de la información estratégica del Estado en materia de Defensa, incluyendo la protección de la infraestructura, las redes estratégicas y la información electrónica; y el fortalecimiento de los mecanismos inter institucionales para hacer frente a las amenazas cibernéticas, por lo que mediante Acuerdo Ministerial No 281, acordó la creación del Sistema de Ciberdefensa del Ministerio de Defensa Nacional como un mecanismo articulador de las instancias pertinentes, para la implementación de las políticas y estrategias de Ciberdefensa a nivel nacional.

Aún no existen convenciones o tratados internacionales que establezcan normas claras sobre la materia. Incluso, en el ciberespacio las tecnologías digitales y las regulaciones se van construyendo a través del tiempo y es posible observar que se diseñan tecnologías para producir los efectos de las regulaciones. Por ello, las estrategias nacionales de defensa y la necesidad de generar nuevas capacidades comenzaron a ser considerados temas centrales y estratégicos dentro de los Ministerios de Defensa y otras agencias gubernamentales. El ciberespacio se anticipa o se vislumbra, desde la perspectiva que interesa a está monografía, como un escenario de conflicto mayor, en el que las actuales escaramuzas, mayoritariamente aun de baja intensidad, pudieran evolucionar a enfrentamientos de mayores dimensiones, que posiblemente combinados con otras actuaciones de fuerza, constituyen una verdadera guerra, la que ha dado en llamarse ciberguerra.

Palabras Clave:

- **CIBERDEFENSA**
- **CIBERESPACIO**
- **CIBERGUERRA**

Abstract

Cyber defense has acquired great worldwide relevance in the last decades. The Ministry of National Defense, established in the National Defense Political Agenda, the need to protect the strategic information of the State in matters of Defense, including the protection of infrastructure, strategic networks and electronic information; and the strengthening of inter-institutional mechanisms to face cyber threats, for which by means of Ministerial Agreement No. 281, it agreed to create the Cyber Defense System of the Ministry of National Defense as an articulating mechanism of the pertinent instances, for the implementation of Cyber defense policies and strategies at the national level. There are still no international conventions or treaties that establish clear rules on the matter. Even in cyberspace, digital technologies and regulations are built over time and it is possible to observe that technologies are designed to produce the effects of regulations. For this reason, national defense strategies and the need to generate new capacities began to be considered central and strategic issues within the Ministries of Defense and other government agencies. Cyberspace is anticipated or seen, from the perspective of interest to this monograph, as a scenario of major conflict, in which the current skirmishes, mostly still of low intensity, could evolve into larger confrontations, which possibly combined with other actions of force constitute a true war, which has come to be called cyberwar.

Keywords:

- **CYBER DEFENSE**
- **CYBERSPACE**
- **CYBER WARFARE**

Capítulo I

El problema.

Planteamiento del Problema.

Es evidente que cuando se habla de Ciberseguridad, el departamento de defensa de los Estados Unidos se refiere al "conjunto de acciones de carácter preventivo que tienen por objeto el asegurar el uso de las redes propias y negarlo a terceros" y más ampliamente se dice que "conjunto de herramientas, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión de riesgos, prácticas idóneas, y tecnologías que pueden utilizarse para proteger los activos de la organización y de los usuarios en el ciberentorno". (DEPARMENT OF THE ARMY UNITED STATES OF AMERICA, 2015-2018)

Para entender la seguridad y defensa desde el contexto del ciberespacio debemos tomar en cuenta dos palabras que podrían confundirse con facilidad: la Ciberseguridad y la Ciberdefensa; la primera de ellas es mucho más amplia, abarca varios ámbitos del Estado y la segunda debe entendérsela como una responsabilidad propia asignada a las Fuerzas Armadas. (Fuertes, Ciberseguridad y Ciberdefensa, 2015)

Los activos de la organización y los usuarios son los dispositivos informáticos conectados, los usuarios, los servicios, aplicaciones, los sistemas de comunicaciones, las comunicaciones multimedios y la totalidad de la información transmitida y/o almacenada en el ciberentorno.[1]

[1] Información del Comando de Ciberdefensa

El ciberespacio en el ámbito mundial, es entendido como el quinto dominio de la guerra, en donde el desarrollo armamentista ya no se enfoca en producir armas, sino utilizando los conocimientos avanzados de las personas conjuntamente con aplicaciones de correlación de información para la toma de decisiones y aplicarla en la ciberguerra, es en ese contexto en el año 2006 el Departamento de Defensa de Estados Unidos, explica que el ciberespacio está caracterizado por el uso de la electrónica y del espectro electromagnético para guardar, modificar, intercambiar información a través de los sistemas y redes de la información y las infraestructuras físicas, por tanto actualmente este escenario es considerado como un dominio global dentro del medio de la información compuesto por las interdependientes infraestructuras y redes de la información, incluyendo internet, las redes de telecomunicaciones, sistemas de computadoras, nuevos dispositivos electrónicos y la información en sí.[2]

Para Badillo, el ciberespacio es entendido como "un sistema de información y proceso de datos interconectados por redes de comunicaciones que involucran el conocimiento humano y tecnológico". (Badillo, Guerra Cibernetica la nueva amenaza, 2011); Mientras que para (Fabregat, 2013), el ciberespacio es un nuevo espacio social múltiple de realidad virtual, compuesto por una matriz de datos digitales, que al estar conectados a nivel mundial hacen que el internauta interrelacione con otros, sin embargo este espacio es dominado por quienes tienen gobierno y control de la web. Bajo ese contexto el ciberespacio se lo define como un espacio virtual, creado por el hombre para transportar información, por medio de redes entre computadores interconectados a nivel mundial. Dicho en otras palabras, el

[2] Información del Comando de Ciberdefensa

ciberespacio es mucho más que el internet, es más que sistemas y equipos, o hardware y software, es un mundo artificial, sin fronteras geográficas del que millones de personas dependen trayendo nuevos retos, riesgos y amenazas.

Las amenazas cibernéticas tienen una connotación diferente a la de otras amenazas a la seguridad del Estado; dado que éstas pueden tener diferentes objetivos, pueden ser realizadas por diferentes tipos de actores como el crimen organizado, terroristas u otros Estados, su costo es mínimo y su trazabilidad es complicada. Bajo ese contexto, la modernización de las Fuerzas Armadas Ecuatorianas se basa en varios ejes estratégicos que entre otros incluye nuevas capacidades operativas como la Ciberdefensa.

Una eficaz reacción para proteger la información y la infraestructura crítica de un país debe sustentarse en una planificación estratégica basada en las capacidades para desarrollar una conciencia situacional del nuevo teatro de operaciones, la naturaleza de las amenazas y la doctrina de empleo de los medios.

Las Fuerzas Armadas deberán orientar su esfuerzo para cumplir con las nuevas capacidades del Comando de Ciberdefensa, combinando las habilidades que se posee para poder asegurar la utilización del ciberespacio, dominio existente dentro del Ambiente informacional que consiste de la red interdependiente de las Tecnologías de Información, Infraestructura e Información residente (base de datos) que permitan bloquear cualquier tipo de amenazas y riesgos en los diferentes escenarios y con diferentes actores provenientes del ciberespacio y que esta organización y el manejo de la Ciberseguridad en Fuerzas Armadas permite emplear al Estado para neutralizar la amenaza del ciberterrorismo a la seguridad.

Formulación del Problema.

El manejo de la Ciberseguridad en las FF. AA, está acorde con las capacidades actuales del COCIBER y sus capacidades específicas necesitan ser revisadas para mejorar su capacidad operativa y luego ser empleada por la Fuerza en las diferentes operaciones, por lo que no se cuenta con una planificación estratégica enfocada hacia dónde están evolucionando las amenazas y riesgos de seguridad en el ámbito global.

Preguntas de Investigación.

1.1.1 ¿Cuál es el escenario prospectivo de FF. AA, frente a las amenazas Cibernéticas y cuáles son las capacidades que tiene el Comando de Ciberdefensa del Comando Conjunto de Fuerzas Armadas?

1.1.2 ¿Cuales son las amenazas y riesgos existentes que debera enfrentar el Comando de Ciberdefensa en el escenario actual?

1.1.3 ¿Se encuentra actualizada la doctrina de ciberdefensa de las Fuerzas Armadas y cual es el marco legal que faculta en realizar operaciones militares en el campo de la ciberdefensa?.

1.1.4 ¿Cuáles serían los requerimientos necesarios para aumentar la capacidad operativa del Comando de Ciberdefensa?

1.1.5 ¿El Comando de Ciberdefensa existen proyectos relacionados a fortalecer la capacidad operativa, de ser así cuales serían los requerimientos para aumentar esta capacidad en contra de las amenazas existentes?

Objeto de Estudio.

El Ministerio de Defensa Nacional, estableció en la Agenda Política de la Defensa Nacional, la necesidad de la protección de la información estratégica del Estado en materia de Defensa, incluyendo la protección de la infraestructura, las redes estratégicas y la información electrónica; el desarrollo de las capacidades de ciber defensa; y, el fortalecimiento de los mecanismos interinstitucionales para hacer frente a las amenazas cibernéticas, por lo que mediante Acuerdo Ministerial No 281 de fecha 24 de septiembre del 2014, acordó la creación del Sistema de Ciberdefensa del Ministerio de Defensa Nacional, como un mecanismo articulador de las instancias pertinentes, para la implementación de las políticas y estrategias de Ciberdefensa a nivel nacional.

La Constitución de la República del Ecuador en su Artículo Art. 158, dispone a las Fuerzas Armadas sean las encargadas de la Seguridad y Defensa del Territorio Nacional, adicional en las reformas constitucionales dadas en el año 2015, ordena el cumplimiento de las operaciones de complementariedad a la Policía Nacional, lo que implica que las Fuerzas Armadas se convierten en una institución de características generales para cumplir las diferentes misiones de seguridad que el Estado Ecuatoriano imponga[3].

"Por mandato de la Constitución de Montecristi, el Ecuador, Estado soberano y democrático, reconoce y garantiza a todas las personas y colectivos, entre otros derechos, los que se refieren a gozar de: una cultura de paz, integridad personal, seguridad humana; protección integral y armonía

[3] Constitución Política de la República del Ecuador de 2008.

con el Buen Vivir del 2011 y hoy en día el Plan toda una Vida con el presidente de la República Lenín Moreno García 2018.

Bajo estas palabras se puede entender que el estado ecuatoriano tiene la obligación de proporcionar a su pueblo una cultura de paz y de seguridad humana, planteando un enfoque de seguridad diferente pero que coloca al ser humano en el centro de su labor para protegerlo de las diferentes consecuencias que puede tener las relaciones internacionales, la justicia, seguridad ciudadana, sistemas de información, riesgos y desastres de origen natural y ocasionados por el hombre.[4]

Se puede observar que el Plan Nacional de Seguridad Integral 2014-2017 (P.N.S.I.) en el CAPÍTULO 14 "POLÍTICAS, ESTRATEGIAS, PROYECTOS Y METAS SECTORIALES DEL CONSEJO DE SEGURIDAD" POLÍTICAS DEL MINISTERIO DE DEFENSA NACIONAL en su política uno," Garantizar la soberanía e integridad territorial, para la consecución del buen vivir, en el marco de los Derechos Humanos", estrategia tres "Desarrollar capacidades para la Ciberdefensa"; en su política cuatro, "Proteger la información estratégica del Estado, en materia de defensa", estrategia uno "Desarrollar acciones de Ciberdefensa que permitan defender la infraestructura crítica, las redes y la información electrónica en el ámbito de la defensa".[5]

Como se puede ver en la Agenda Política de la Defensa 2014-2017, se exhorta como otro elemento fundamental para el fortalecimiento de las Fuerzas Armadas para la defensa y desarrollo nacional, el apoyo que el

[4] Plan Nacional de Seguridad Integral 2014-2017.
[5] Plan Nacional de Seguridad Integral 2014-2017.

gobierno debe de entregar para la modernización de la institución armada y en la que por obligación poseen los miembros de la misma. Además, induce al fortalecimiento de las operaciones de protección del espacio cibernético.[6]

En las políticas y estrategias de la defensa, en los ámbitos de la defensa incluyen un numeral 2 denominado “Militar”, que debe existir un nuevo diseño de las Fuerzas Armadas en el cual se involucre una adecuación de marcos conceptuales que estén orientados a ser innovadores y armónicos orientados a las nuevas realidades existentes, especialmente a todos los ámbitos donde se encuentre la tecnología y que se transforme en un factor multiplicador de las capacidades estratégicas, para poder combatir a las nuevas amenazas que atenten el bienestar del Estado y sus conciudadanos.

La Agenda[7] establece los siguientes campos donde Fuerzas Armadas se empleará:

- Defensa de la Soberanía y la Integridad Territorial.
- Apoyo a la Acción del Estado.
- Apoyo al desarrollo Nacional.
- Cooperación Internacional.

Todo esto que se ha mencionado hace que el Ministerio de Defensa Nacional elabore la Directiva de Defensa Nacional y en ella se crean políticas y estrategias encaminadas al desarrollo de las capacidades de la institución; Las mismas son las siguientes:

[6] Agenda de la Política de la Defensa 2014-2017.
[7] Agenda de la Política de la Defensa 2014-2017.

a. Alcanzar una capacidad de defensa militar que permita respaldar las acciones del Estado ante potenciales controversias:

    1) Fortalecer operativamente a las FF. AA con capacidades estratégicas conjuntas.
    2) Incrementar la capacidad de prevención, disuasión y defensa ante cualquier tipo de amenaza y/o desastres.
    3) Mejorar la capacidad de vigilancia, control y respuesta efectiva del territorio continental e insular, espacios acuáticos y espacio aéreo.

b. Apoyar a las acciones del Estado en seguridad interna en el marco de las competencias específicas de las Instituciones:

    1) Mejorar la capacidad de protección de la población, los recursos y el patrimonio nacional.
    2) Desarrollar nuevas capacidades, sin desatender las misiones principales, con un respaldo legal adecuado.
    3) Elaborar y proponer las reformas legales, educativas, organizacionales y presupuestarias para asumir las misiones subsidiarias."[8]

El Ministerio de Defensa Nacional velará por el fortalecimiento de las capacidades operativas pertinentes y desarrollará las políticas específicas en el ámbito aeroespacial, Ciberdefensa, gestión de riesgos, seguridad integral,

[8] Directiva de la Defensa Militar 2012

empleo progresivo de la fuerza contra vuelos ilegales y misiones de inteligencia.[9]

Campo de Acción.

El Comando de Ciberdefensa del Comando Conjunto, busca cumplir su misión dentro de tres líneas de operaciones primarias: asegurar, operar y defender el Sistema de Información del Comando Conjunto (SICC)[10], defender a las instalaciones estratégicas críticas de la nación de ataques cibernéticos y proporcionar apoyo cibernético a los Comandos Operacionales que lo requieran. Para ello dispone de personal y unidades entrenadas y equipadas para realizar operaciones en el ciberespacio (OC)[11].

Relaciones de comando claramente establecidas son cruciales para asegurar un empleo oportuno y efectivo de las fuerzas, y las OC requieren de unidad de comando y unidad de esfuerzo. Sin embargo, la naturaleza compleja de las OC, donde las fuerzas del ciberespacio pueden estar proporcionando simultáneamente acciones en el nivel nacional y en el nivel de teatro, por lo que se requiere una adaptación de las estructuras tradicionales de C2. Las fuerzas conjuntas, emplean principalmente la planificación centralizada con una ejecución descentralizada de las operaciones.

Las Operaciones de Ciberespacio (OC), requieren una coordinación constante y detallada entre las operaciones nacionales y de teatro, creando

[9] Agenda Política de la Defensa 2014-2017
[10] Sistema de Información del Comando Conjunto (SICC)
[11] Operaciones en el Ciberespacio (OC)

una estructura dinámica de C2[12] que se pueda adatar a los cambios constantes, amenazas emergentes y desconocidas. Ciertas funciones de las Operaciones de Ciberespacio, incluyendo la protección de las redes de Network del Sistema de Información del Comando Conjunto (SICC), así como la búsqueda de las múltiples amenazas, orientan a la planificación y ejecución centralizada para alcanzar los requerimientos múltiples e instantáneos de respuesta. Las OC deben estar integradas y sincronizadas por el comandante apoyado dentro de su concepto operacional, planes y órdenes detallados y en las operaciones conjuntas específicas.

Delimitación de la Investigación

Delimitación Temática.

La realización del presente estudio permitirá determinar un mecanismo articulador entre la doctrina y las capacidades que podrían minimizar las posibles amenazas y riesgos existentes en el manejo de la Ciberseguridad en las Fuerzas Armadas, a fin de establecer los lineamientos doctrinarios ante la necesidad de la protección de la información estratégica del Estado en materia de Defensa y Seguridad.

Delimitación Espacial.

Esto se desarrollará en el marco del contexto nacional, analizando las capacidades en el Ciberespacio que posee el comando de Ciberdefensa en cuanto a las amenazas y riesgos existentes en el País, así como las acciones que debe tomar las Fuerzas Armadas ecuatorianas para la defensa de la Seguridad Nacional.

[12] C2: Comando y Control

Delimitación Temporal.

Para el presente trabajo de investigación se considerará los diferentes eventos suscitados desde el año 2015 hasta la presente fecha.

Justificación de la Investigación.

Originalidad

Todo lo anterior conlleva a crear una obligación en Fuerzas Armadas, que es proteger la información y la infraestructura crítica. Para que las Fuerzas puedan cumplir su cometido en bien del pueblo ecuatoriano; por ende, se tiene que conocer las diferentes capacidades que un Comando de Ciberdefensa debe poseer para cumplir con su objetivo propuesto. Se tiene que conformar un Comando de Ciberdefensa con capacidades de enfrentar a cualquier tipo de amenaza que se presente en el ciberespacio. La Fuerzas Armadas requieren tener claramente determinadas las misiones y procedimientos que se deberán cumplir ante los problemas que genera la seguridad de las tecnologías de información en FF. AA.

Relevancia

La Seguridad en los Estados ha ido cambiando de acuerdo a las situaciones que van desarrollando dentro de él y dentro de su entorno, es así que en los últimos 20 años, la informática ha evolucionado mucho, pasando de ser una herramienta administrativa para optimizar procesos de oficina a un instrumento estratégico para la industria, la administración y las Fuerzas Armadas. Antes del 11-S los riesgos y retos de seguridad cibernéticos sólo se

trataban dentro de pequeños grupos de expertos, pero a partir de esa fecha resultó evidente que el ciberespacio introduce graves vulnerabilidades en unas sociedades cada vez más interdependientes. Es así como se ve comprometido toda la nación y en general al mundo global, ya que se ha evidenciado que esto es un punto neurálgico y que es vulnerable para la soberanía de los estados, por esta razón este tema es de vital importancia e interés para FF. AA.

Interés

El presente trabajo se enmarca en bien de los intereses institucionales de Fuerzas Armadas, debido a que en la actualidad no solo se enfrenta a un enemigo conocido sino a diferentes amenazas y riesgos que se presentan con el desarrollo de la humanidad. El saber utilizar la información y aprovechar ésta, obliga a tener un organismo que se encargue de proteger las redes y sistemas informáticos de Fuerzas Armadas y su infraestructura crítica, constituyéndose en parte fundamental para el éxito de las operaciones en cualquier tipo de escenario, es por esto, que la guerra de la información se ha convertido en una nueva generación de los conflictos dentro de un país o de una región que entra en esta situación.

Las Fuerzas Armadas tienen la misión constitucional de defender la soberanía y ser los encargados de la Defensa Nacional, en tal virtud, deberán planificar y ejecutar operaciones encaminadas a neutralizar las amenazas anteriormente descritas, enmarcadas en políticas claras y con leyes que respalden su accionar.

Factibilidad

Siendo de interés nacional y al tener como participantes a las Fuerzas Armadas y al ser un fenómeno actualmente palpable es necesario conocer y saber cómo están operando las capacidades del Comando de Ciberdefensa, para desde nuestro nivel contribuir con la seguridad de la información, y de interés profesional y con el apoyo analítico de los instructores de la Academia de Guerra, se puede construir un documento que ayudará a fortalecer no solamente al Comando de Ciberdefensa sino a la Institución. Además, se puede indicar que el tema propuesto es de interés institucional, porque la transmisión y recepción de la información de Fuerzas Armadas, fluye a través de la red estratégica de comunicaciones de Fuerzas Armadas (MODE), la misma que tiene acceso a la internet, convirtiéndose en una red vulnerable para los hackers y crackers de las redes informáticas.

Objetivos de la Investigación.

Objetivo General.

Desarrollar una guía doctrinaria para el Comando de Ciberdefensa, para que de manera integrada y coordinada permita definir aquellos aspectos que deben ser considerados en base a las capacidades actuales del COCIBER, para contribuir en el mejoramiento de la capacidad operativa del Comando de Ciberdefensa del CC.FF.AA, ante las nuevas amenazas y riesgos del ciberespacio, así como la de proponer una política y estrategias para neutralizar la amenaza del ciberterrorismo contra la seguridad del Estado.

Objetivos Específicos.

a. Analizar el escenario prospectivo de Fuerzas Armadas en el campo de la Ciberdefensa.

b. Analizar los aspectos doctrinarios que deber ser tomados en consideración para el desarrollo de las capacidades del ciberespacio.

c. Analizar la planificación por capacidades del Comando Conjunto de las FF.AA.

d. Determinar las amenazas y riesgos existentes para el Comando de Ciberdefensa.

e. Determinar los requerimientos necesarios para aumentar la capacidad operativa del Comando de Ciberdefensa.

Capítulo II

MARCO TEÓRICO.

Antecedentes de la Investigación.

Si se retrocede en la historia nos damos cuenta que, con el fin de la Guerra Fría, marcaron una nueva etapa democrática en la seguridad del Estado Ecuatoriano y a raíz del año 2011, donde se presenta al país un nuevo enfoque a la seguridad Integral, la cual conceptúa unas nuevas amenazas basadas en el espectro electromagnético Multidimensional, ciberespacio y al disponernos el cumplimiento de nuevos roles y tareas a través de la Agenda Política de la Defensa.

Es fundamental que todo el personal militar entienda y tenga totalmente claro lo que establece en la actualidad desde nuestra Constitución de la República en los artículos: 3, 66, 147, 158, 261 y 393; así como también las nuevas misiones asignadas a las Fuerzas Armadas que son “Garantizar la Defensa de la Soberanía e Integridad Territorial” “Participar en la Seguridad Integral” “Apoyar al Desarrollo Nacional en el ejercicio de las Soberanías” y “Contribuir a la paz regional y mundial”; mencionando además que constituye una institución de protección de derechos, libertades y garantías de los ciudadanos. (Asamblea Nacional Constituyente, 2008)

El Plan Nacional de desarrollo Toda una Vida 2017-2021, constituye la normativa que determina nueve objetivos nacionales para el Buen Vivir, así como las políticas y lineamientos estratégicos para construir una sociedad más justa. (SENPLADES, 2016); El Plan Nacional de Seguridad Integral

2017-2021, establece dos políticas intersectoriales para el sector Defensa, los cuales se relacionan con 5 objetivos nacionales del Buen Vivir (objetivos 2, 3, 6, 7, 9), ((Ministerio Coordinador de Seguridad, 2016); ya que al conocer todo lo planteado anteriormente el personal militar e inclusive el personal de servidores públicos que laboran en las Fuerzas Armadas estarán en condiciones de dar cumplimiento a las nuevas misiones asignadas, a los nuevos objetivos planteados para la institución y más aún que nuestro personal esté preparado para asumir y enfrentar estos nuevos retos que el gobierno de turno no ha asignado, demostrando de esta manera el profesionalismo que caracteriza a los soldados de honor, cumplidores de las normas y procedimientos que establecen las leyes de la república.

Por otra parte, en la Ley de Seguridad Pública y del Estado expresa en su Art. 11. Los órganos ejecutores del Sistema de Seguridad Pública y del Estado estarán a cargo de las acciones de defensa, orden público, prevención y gestión de riesgos, conforme lo siguiente: a) De la defensa: Ministerios de Defensa, Relaciones Exteriores y Fuerzas Armadas. - La defensa de la soberanía del Estado y la integridad territorial tendrá como entes rectores al Ministerio de Defensa y al de Relaciones Exteriores en los ámbitos de su responsabilidad y competencia. Corresponde a las Fuerzas Armadas su ejecución para cumplir con su misión fundamental de defensa de la soberanía e integridad territorial[13]. (seguridad, 2014).

La mayoría de las acciones del ciberespacio utilizan el ciberespacio para facilitar otros tipos de actividades, que emplean las capacidades del ciberespacio para completar otras tareas que no son parte de las tres

[13] Ley de Seguridad Pública y del Estado, Art 11

misiones de las Operaciones del Ciberespacio: Operaciones Ofensivas en el Ciberespacio, Operaciones Defensivas en el Ciberespacio y las operaciones del Comando Conjunto.

Esa utilización incluye acciones como la operación de un sistema de C2 o de un sistema logístico, él envió de un email para apoyar un objetivo de información, el uso del internet para completar un curso de entrenamiento online, o para desarrollar un briefing. Otros usuarios, que pueden ser usuarios no autorizados de network, personal del Comando Conjunto que no necesita una autorización especial para utilizar las capacidades del ciberespacio, etc. En el ciberespacio la mayoría de las vulnerabilidades del sistema del Comando Conjunto, pueden estar expuestas y ser explotadas por nuestros adversarios. El desafío es entrenar a todos los usuarios del Comando Conjunto para comprender el significado de las amenazas del ciberespacio, y a reconocer las tácticas de la amenaza para que el uso del ciberespacio no genere un riesgo innecesario a las operaciones. La protección del ciberespacio del Comando Conjunto mediante el establecimiento de una cultura de prevención de las vulnerabilidades, particularmente mediante políticas, prácticas y entrenamiento, es crítico para el éxito de todos los tipos de operaciones permitidas en el ciberespacio.

El Ministerio de Defensa Nacional velará por el fortalecimiento de las capacidades operativas pertinentes y desarrollará las políticas específicas en el ámbito aeroespacial, Ciberdefensa, gestión de riesgos, seguridad integral, empleo progresivo de la fuerza contra vuelos ilegales y misiones de inteligencia.[14]

[14] Agenda Política de la Defensa 2014-2017

Fundamentación teórica.

El Comando Conjunto de las Fuerzas Armadas ante las situaciones impuestas por el Estado realiza su planificación mediante el Plan Estratégico Institucional de Fuerzas Armadas 2010 - 2021, en el documento se encuentra detallado los procedimientos a seguir para alcanzar la excelencia profesional de la institución, orientada al aprovechamiento de las capacidades específicas para la consecución de las capacidades estratégicas, mediante la ejecución del cumplimiento de objetivos estratégicos y estrategias específicas. Estas capacidades específicas planteadas son las siguientes:

a. Incrementar el nivel de imagen, credibilidad y confianza en Fuerzas Armadas.

b. Incrementar la participación de Fuerzas Armadas en programas de apoyo al desarrollo nacional, con responsabilidad social.

c. Incrementar la capacidad de cooperación con los organismos de seguridad interna del Estado.

d. Incrementar la presencia internacional de personal y unidades militares en operaciones de mantenimiento de la paz, ayuda humanitaria y fomento de la confianza y seguridad mutua.

e. Incrementar la capacidad de vigilancia, control, alarma temprana y defensa de la soberanía e integridad territorial.

f. Incrementar el alistamiento operacional de FF.AA.

g. Incrementar las capacidades estratégicas conjuntas de FF.AA.

h. Incrementar la gestión institucional por resultados

i. Incrementar las competencias y fortalezas del talento humano en un adecuado clima laboral.

j. Incrementar los niveles de desarrollo tecnológico y el fortalecimiento de la investigación de Fuerzas Armadas. "[15]

El Comando Conjunto se ha visto en la obligación de crear diferentes programas que fortalezcan y se ejecuten en base a los objetivos a alcanzar, todo esto realizado sobre los presupuestos asignados, pero siendo claros que la algunos de estos no se pueden cumplir en un tiempo corto, lo que obliga a una planificación por prioridades y apoyadas en el Plan Capacidades Estratégicas Conjuntas.

Las áreas de capacidades conjuntas del Comando Conjunto de las Fuerzas Armadas se materializan en las siguientes:

a. Mando y Control

b. Vigilancia, Reconocimiento, Inteligencia y Adquisición de Objetivos.

c. Maniobra.

d. Despliegue y Movilidad

e. Supervivencia y Protección.

f. Sostenimiento logístico[16]

[15] Plan Estratégico de Fuerzas Armadas 2010-2021

[16] Plan de Gestión Institucional del CC. FF. AA 2010 - 2021

Cabe señalar que de acuerdo al documento del Sistema de Planeamiento por Capacidades del CC.FF.AA. 2015, se incrementa una capacidad más, el apoyo a la gestión del estado, es decir, actualmente son siete capacidades del CC.FF.AA.[17]

En el área de capacidad de Mando y Control se encuentra la capacidad de Protección de la Información (Ciberdefensa), cuyo objetivo es proteger la información contra accesos no autorizados y evitar que esta información sea modificada o manipulada, tanto cuando está almacenada, como cuando se está procesando o en tránsito, y contra la denegación de acceso a usuarios autorizados, incluyendo aquellas medidas necesarias para detectar, documentar y hacer frente a tales amenazas.

[17] Sistema de Planeamiento por Capacidades del CC.FF.AA.2015

Fundamentación General

El Ministerio de Defensa Nacional, estableció en la Agenda Política de la Defensa Nacional, la necesidad de la protección de la información estratégica del Estado en materia de Defensa, incluyendo la protección de la infraestructura, las redes estratégicas y la información electrónica; el desarrollo de las capacidades de Ciberdefensa; y, el fortalecimiento de los mecanismos inter institucionales para hacer frente a las amenazas cibernéticas, por lo que mediante Acuerdo Ministerial No 281 de fecha 24 de septiembre del 2014, acordó la creación del Sistema de Ciberdefensa del Ministerio de Defensa Nacional, como un mecanismo articulador de las instancias pertinentes, para la implementación de las políticas y estrategias de Ciberdefensa a nivel nacional.

La autoridad para la planificación ejecución de Operaciones militares en el ciberespacio está establecida dentro de las políticas emitidas por el Ministerio de Defensa, así como en las órdenes recibidas que autorizan al Comando de Ciberdefensa a la ejecución de estas operaciones.

Fundamentación Específica

a. **Escenario prospectivo de FF. AA en diferentes escenarios de varios países.**

Actualmente el Comando Conjunto de las Fuerzas Armadas se encuentra frente a un entorno complejo, incierto y dinámico y es justamente en esa incertidumbre cuando funciona la prospectiva, que es la herramienta utilizada para el diseño del escenario de las Fuerzas Armadas ecuatorianas. Si bien el futuro

es imposible de predecir, la prospectiva es una disciplina científica que nos ayuda a reducir la incertidumbre y desentrañar el futuro, si bien es una disciplina relativamente nueva en nuestro medio, en el mundo se viene aplicando desde inicios del siglo XX.[18]

La prospectiva ha sido empleada por gobiernos de varios países, no obstante, es en el campo empresarial donde ha tenido un impacto significativo. En la actualidad, las grandes empresas internacionales, bancos, compañías de negocios y los grandes ejércitos, emplean la prospectiva para el planeamiento de mediano y largo plazo de sus operaciones.

En la actualidad, ya no es posible realizar solo el planeamiento estratégico tradicional, ni en lo político, ni en lo empresarial, ni en lo militar, basados en una "visión" única y siempre deseable para las instituciones; sino que es preciso contar con estrategias claras, además de planes de contingencia basados en diferentes escenarios alternativos, posibles y probables, es aquí donde la prospectiva produce su mayor beneficio.

b. Planificación por capacidades del CC. FF. AA, mejor rendimiento, mejor organización de las unidades

La planificación basada en capacidades aplicada por Fuerzas Armadas ecuatorianas proporciona un fundamento más

[18] Plan de Gestión Institucional de FF. AA 2010 - 2021

racional para la toma de decisiones sobre la modernización del material existente, adquisiciones futuras y el sostenimiento operacional, a la vez que ofrece soluciones integrales, para afrontar con éxito los actuales y potenciales escenarios de conflicto. El objetivo general del Plan de Capacidades es enfocar las operaciones militares hacia la acción conjunta para conseguir la máxima eficacia en los resultados, evitando las necesidades y soluciones aisladas y no orientadas a la consecución de los objetivos estratégicos de FF.AA. Considerando que capacidad se define como la aptitud o suficiencia específica que le permite a una organización cumplir con su misión básica y sus funciones, las capacidades que deben tener las Fuerzas Armadas ecuatorianas han sido determinadas por capacidades estratégicas y capacidades específicas, las cuales les permitirán cumplir con la misión constitucional y con las misiones subsidiarias asignadas.[19]

El nuevo diseño de Fuerzas, debe responder al desarrollo de capacidades para el empleo conjunto de las Fuerzas Armadas, para enfrentar con éxitos las amenazas, riesgos y desafíos del Estado, en los actuales y futuros escenarios estratégicos de seguridad y defensa, así como en las amenazas emergentes.

c. Amenazas y riesgos del Comando de Ciberdefensa

La multiplicidad de potenciales atacantes incrementa los riesgos y amenazas que pueden poner en graves dificultades los

[19] Plan de Gestión Institucional de FF. AA 2010 - 2021

servicios prestados por las Administraciones Públicas, las infraestructuras Críticas o las actividades de las empresas y ciudadanos. Además, existen evidencias de que determinados países disponen de capacidades militares y de inteligencia para realizar ciberataques que ponen en riesgo la Seguridad Nacional.[20]

La Ciberseguridad es una necesidad de nuestra sociedad y de nuestro modelo económico. Dada la influencia de los Sistemas de Información y Telecomunicaciones en la economía y en los servicios públicos, la estabilidad y prosperidad de Ecuador depende en buena medida de la seguridad y confiabilidad del ciberespacio, cualidades que pueden verse comprometidas por causas técnicas, fenómenos naturales o agresiones deliberadas.

d. Requerimiento para aumentar la capacidad operativa

El Comando de Ciberdefensa hasta el 2017, pretende encontrarse en lo referente a personal a un porcentaje del 50% (45 de 89) del disponible en relación al orgánico. En cuanto a Oficiales al 50% (9 de 18 Oficiales), en lo referente a personal de Tropa al 50% (33 de 66 Voluntarios, Tripulantes y/o Aerotécnicos) y en cuanto a Servidores Públicos al 20% (1 de 5 Servidores Públicos).

[20] Estrategias de Ciberseguridad Nacional 2013 España

Se considera que a finales del año 2017 sus capacidades se incrementarán a la ejecución de acciones de defensa, exploración y respuesta ante incidentes o amenazas que se produzcan en el ciberespacio, que puedan atentar a la infraestructura crítica de Fuerzas Armadas, incrementando el porcentaje de operatividad al 75%.

En lo referente a la operabilidad, el Comando de Ciberdefensa, una vez que ha iniciado su implementación, parte con un porcentaje de sus capacidades al 5 % y una vez implementado el proyecto a fines del 2017 aspira alcanzar un 75 % de sus capacidades, tendiente a proteger la infraestructura crítica digital de Fuerzas Armadas.[21]

Base Legal

Cuando se refiere a la seguridad de un estado, se debe entender que estamos hablando de la política de defensa nacional y de esta manera del libro blanco, que es quien da los lineamientos necesarios para el accionar de las Fuerzas Armadas, este momento se está elaborando el libro blanco del año 2018. Por otra parte hay que considerar la perspectiva, es decir tener una visión estratégica, de determinar los principales escenarios, si hay un análisis de los escenarios futuros, se podrán tomar decisiones acertadas, caso contrario, no se podrá planificar, sino se tiene la certeza de estar en las condiciones operativas, lo más probable es que no se tenga éxito en la operación, por consiguiente una visión estratégica de un comandante es muy importante para la toma de decisiones y como dirigirlas, el principal

[21] Apreciación del Comando de Ciberdefensa del CC. FF. AA

documento que orienta las actividades de las Fuerzas Armadas es la Constitución de la República del Ecuador ya que en su Art 158, nos dice: “Las Fuerzas Armadas tienen como misión fundamental la defensa de la soberanía y la integridad territorial. (Constitución, 2008).

Se conoce las capacidades que tiene las Fuerzas Armadas, además conocemos la amenazas y que es lo que quieren realizar estas amenazas y así podemos determinar que podemos realizar, adicional es muy importante la inteligencia, para conocer las intenciones de las amenazas y poder neutralizarla, en la ley orgánica de la defensa Nacional en su Art. 2. Nos dice: “Las Fuerzas Armadas, como parte de la fuerza pública, tienen la siguiente misión: a) Conservar la soberanía nacional; b) Defender la integridad, la unidad e independencia del Estado; y, c) Garantizar el ordenamiento jurídico y democrático del estado social de derecho. Además, nos expresa que debemos colaborar con el desarrollo social y económico del país; se podrán participar en actividades económicas relacionadas exclusivamente con la defensa nacional; e, intervenir en los demás aspectos concernientes a la seguridad nacional, de acuerdo con la ley”. (Orgánica, 2007).

- La Constitución de la República del Ecuador de 2008 en su Artículo Art. 158, nos dice: “Las Fuerzas Armadas sean las encargadas de la seguridad y defensa del territorio nacional.[22].
- Mediante Orden Ministerial No 188 del 24 de septiembre de 2014, se cree el Comando de Ciberdefensa[23].
- Agenda de la Política de la defensa en donde se establecen los campos de acción donde Fuerzas Armadas se emplearán.

[22] Constitución Política de la República del Ecuador de 2008.
[23] Orden Ministerial No 188 del 24 de septiembre de 2014

- Plan Nacional de Seguridad Integral 2017 – 2021[24].
- Para el cumplimiento de competencias, deberes y responsabilidades en todo el ámbito nacional, el Ecuador utiliza como guía determinante un marco legal establecido, la Constitución de la República, en su Artículo 158 define como misión fundamental de Fuerzas Armadas la defensa de la soberanía y la integridad territorial.

Hipótesis

La existencia de una guía doctrinaria integrada y coordinada con las capacidades del Comando de Ciberdefensa del CC.FF.AA, permitirán enfrentar las nuevas amenazas y riesgos del Ciberespacio, así como las Políticas y Estrategias para neutralizar la amenaza del Ciberterrorismo contra la seguridad del Estado.

Sistema de Variables

Variables Independientes.

- Análisis de las Capacidades del Comando de Ciberdefensa del Comando Conjunto de las FF. AA, referente a las políticas y estrategias de seguridad ante las amenazas y riesgos existentes.
- Misiones de las Fuerzas Armadas ante estas amenazas y riesgos existentes.
- Escenario prospectivo de FF. AA,
- planificación por capacidades del CC.FF.AA. y
- Capacidades del Comando de Ciberdefensa

[24] Plan Nacional de Seguridad Integral 2017 – 2021

Variables dependientes.

- Marco regulatorio para neutralizar las amenazas y riesgos del Ciberterrorismo contra la seguridad del Estado.

Conceptualización y Operacionalización de las variables

Conceptualización y Operacionalización de las variables independientes.

VARIABLE	CONCEPTUALIZACIÓN	DIMENSIONES	INDICADORES	TÉCNICAS E INSTRUMENTOS DE RECOLECCIÓN DE INFORMACIÓN
Escenario prospectivo de FF. AA	Un escenario muestra un futuro posible o eventos posibles, compaginando las imágenes que muestran el resultado de las acciones que se tomará, entonces cada una de estas imágenes influirán en el porvenir.	• Escenarios. • Ciberespacio	• Número de escenarios previstos.	• Escenarios • Tendencias • Análisis de encuestas
Planificación por capacidades del CC.FF.AA.	El Planeamiento por Capacidades es un proceso de planeamiento, más adecuado al entorno estratégico y que hace posible el diseño de las Fuerzas, así como la obtención de los medios y recursos necesarios para la consecución de las capacidades militares para alcanzar los objetivos establecidos desde el nivel político.	• Las Fuerzas. • Unidades.	• Mejor rendimiento. • Mejor desempeño • Organización de las unidades.	• Encuesta. • Entrevistas. • Observación Sistemática.

Capacidades del Comando de Ciberdefensa.	Capacidad Militar para proteger la información contra accesos no autorizados y evitar que esta información sea modificada o manipulada, tanto cuando está almacenada, como cuando se está procesando o en tránsito, y contra la denegación de acceso a usuarios autorizados, incluyendo aquellas medidas necesarias para detectar, documentar y hacer frente a tales amenazas.	• Personal militar e instalaciones del Comando de Ciberdefensa. • Fuerzas • Unidades	• Responsabilidades cumplidas / Responsabilidades planificadas.	• Fuentes abiertas. • Encuesta • Investigación bibliográfica • Revisión Bibliográfica
Amenazas y riesgos del Comando de Ciberdefensa.	Entendiéndose como amenaza y riesgos a toda persona o grupo de personas organizadas, circunstancia o situación que ponga en peligro la infraestructura crítica de FF.AA.	• Tipo de amenaza o riesgos. • Sector de desarrollo de la amenaza o riesgos. • Incidencia y consecuencias de las amenazas y riesgos.	• Amenazas externas. • Amenazas internas. • Factores de riesgo. • Incremento de los ciberataques. • Hackers y crackers	• Encuesta. • Entrevistas. • Observación Sistemática. • Escala de actitudes.

Requerimientos para aumentar la capacidad operativa.	Son los medios que se necesitan en lo referente a software, hardware y recursos humanos capacitados que se requiere para aumentar la capacidad operativa del Comando de Ciberdefensa.	• Sistemas de seguridad y defensa • Recursos humanos • Capacitación • Presupuesto	• Planificación de operaciones de Ciberseguridad. • Cantidad de ataques a la red. • Estructura Organizacional Estratégica. • Bloqueos de ataques cibernéticos. • Personal idóneo para Ciberdefensa.	• Encuestas • Observación sistemática. • Monitoreo.

Conceptualización y Operacionalización de las variables dependientes.

VARIABLE	CONCEPTUALIZACIÓN	DIMENSIONES	INDICADORES	TÉCNICAS E INSTRUMENTOS DE RECOLECCIÓN DE INFORMACIÓN
Marco regulatorio para la guía, control y gestión de un sistema de Ciberseguridad nacional que posibilite neutralizar las amenazas y riesgos en espacio electromagnético	Conjunto de reglas que forman la base de las regulaciones que permitan proteger la seguridad de los usuarios del ciberespacio, proteger la seguridad del país, promover la coordinación y cooperación entre las instituciones y gestionar los riesgos del ciberespacio.	• Normativa Política	• Normativa para implementar la Ciberseguridad en el Estado. • Normativa para gestionar la Ciberseguridad en las instituciones públicas y privadas.	• Escenarios • Tendencias • Análisis de encuestas. • Revisión Bibliográfica.
		• Amenazas y riesgos	• Amenazas a la Ciberseguridad. • Riesgos a la Ciberseguridad. • Porque debe existir una seguridad integral para eliminar estas amenazas existentes en el país.	• Encuesta. • Entrevistas. • Revisión Bibliográfica.
		• Sistema de Ciberseguridad	• Responsabilidades cumplidas / Responsabilidades planificadas.	• Fuentes abiertas. • Encuesta • Revisión Bibliográfica

Capítulo III

MARCO METODOLÓGICO.

Enfoque de la Investigación.

La investigación se fundamentará y se justificará en nuestro estudio en función de los objetivos y propósitos que hemos planteado, este trabajo tiene carácter de investigación en el campo de la Ciberdefensa y sobre todo en la seguridad del Estado frente a las amenazas y riesgos existentes, en la que interpretaremos los datos investigados y de las opiniones de especialistas que nos ayudarán a dar un correcto enfoque de esta investigación.

Este escenario muestra un futuro posible o futuros posibles, compaginando las imágenes que muestran el resultado de las acciones a tomar, entonces cada una de estas imágenes influirán en el futuro. Por lo tanto, los escenarios descritos servirán para decidir lo que vamos hacer en el presente, cumpliendo las siguientes condiciones de pertinencia, coherencia, verosimilitud, importancia y transparencia. (Astigarraga, 2016)

Mientras que Freire B, “Un escenario es una imagen o visión que describe una situación futura así como la secuencia de eventos que permiten llegar a esa situación. Este método, permite, entonces, transitar desde la situación actual hasta otra situación futura, deseable y posible, describiendo coherentemente dicho tránsito”. (Freire, 2016)

Para este estudio se comprende por escenario al conjunto de eventos que se tendrán que enfrentar en un determinado lugar geográfico, con condiciones impuestas por las situaciones dadas en un determinado tiempo y con los medios que nos sirvan para cumplir la misión.

Una capacidad, es un conjunto de recursos que con las actitudes de una persona o grupo de personas se desarrollan en bien del cumplimiento de una tarea o cometido.

Una capacidad militar comprende un conjunto de factores comprendidos en: sistemas de armas (equipo material), infraestructura, personal y medios (combate y apoyo logístico), asentados sobre la base de unos principios y procedimientos doctrinales que pretender conseguir un determinado efecto militar a nivel estratégico, operacional o táctico, para cumplir con las misiones asignadas.[25]

"Para explicar lo que se ha denominado como un "Planeamiento Basado en Capacidades", primero hay definir qué se entiende por Capacidad. En términos militares, es el conjunto de factores (sistemas de armas, infraestructura, personal y medios de apoyo logístico) asentados sobre la base de unos principios y procedimientos doctrinales que pretenden conseguir un determinado efecto militar a nivel estratégico, operacional o táctico, para cumplir las misiones asignadas. Es decir, una Capacidad Militar no es únicamente un arma o un

[25] Comando de Educación y Doctrina del Ejército 2018

sistema de armas, sino un conjunto de factores, más o menos críticos, pero todos igualmente importantes para la consecución del efecto deseado."[26]

Para la presente investigación se definirá a las capacidades como el conjunto de factores (sistema de armas, infraestructura, personal y medios), que, asentados sobre la base de principios y procedimientos doctrinarios pretenden conseguir un determinado efecto militar, imprescindible, para el cumplimiento de las misiones asignadas a las Fuerzas Armadas.

Se puede considerar como amenaza a "aquel fenómeno o proceso natural, causado por el ser humano que puede poner en peligro a una persona, grupo, comunidad, estado o la comunidad internacional".[27]

De acuerdo a lo que enuncia (Pérez, 2018), todos los componentes que estructuran el ciberespacio y sus diferentes amenazas se constituyen en riesgos latentes para los individuos y los estados, sobre todo las grandes naciones que dependen en un 80% de su manejo tecnológico a través de redes.

Las amenazas cibernéticas tienen una connotación diferente a la de otras amenazas a la seguridad del Estado; dado que éstas pueden tener diferentes objetivos, pueden ser realizadas por diferentes tipos de actores como el crimen organizado, terroristas u otros Estados, su costo es mínimo y su trazabilidad es complicada.

[26] Planeamiento por Capacidades, Revista Española de Defensa, junio 2017
[27] Concepto de Amenaza del Manual de Defensa Interna MIP-10-01-2010, CEDE

Durante los últimos años, las naciones se han visto obligadas a actualizar sus Estrategias Nacionales de Seguridad y Defensa hacia un nuevo escenario que es el CIBERESPACIO debido a las diversas razones que han producido un incremento de Amenazas y Riesgos[28]:

La tecnología y el espectro electromagnético es la base del ciberespacio, y también sobre la que se apoyan las principales amenazas de éste y en éste. Un enfoque tecnológico del ciberespacio da cabida a las dos visiones previas, tanto la pesimista como la optimista. Tan cierto es que las amenazas crecen, se especializan y sofistican sus métodos de manera continua, como que las ventajas que aporta el ciberespacio, y las herramientas de defensa de las que se dispone, y no sólo tecnológicas, permiten asegurar que este es un medio irrenunciable que establece un nuevo paradigma de cohesión mundial.

Néstor Ganuza, asegura que los riesgos cibernéticos son numerosos, entre los que destacan, una complicada actividad criminal desarrollada por grupos organizados o delincuentes individuales; quienes utilizan el ciberespacio grandemente para sus acciones terroristas y el apoyo a ellas; una mayor y más compleja actividad de espionaje, ya sea industrial, militar o político; una gran cantidad de ataques a las infraestructuras críticas nacionales, a las libertades públicas y a todo tipo de servicios en los que se basa el funcionamiento de las sociedades modernas; una mayor participación de ciudadanos particulares en acciones maliciosas, ya sea por ignorancia, por curiosidad, por diversión, por

[28] "AMENAZAS INFORMÁTICAS EN LA WEB 3.0": Guía para aprender a identificar y prevenir los riesgos a los que usted y su familia, se exponen, al navegar en Internet, Félix A. Reyes G. y Carlos Andrés Lugo González, (Spanish Edition) Kindle Edition, 15 de Agosto 2017

reto o por lucro; esto ha ocasionado muchos riesgos como causa de la atracción que el ciberespacio produce al ofrecer una mayor rentabilidad, globalidad, facilidad e impunidad para todo este tipo de actividades. (GANUZA, 2015)

De acuerdo al estudio del uso de internet y las nuevas tecnologías 2018, sitúa a usuarios con y sin recursos en un plano equivalente, es decir usuarios con menores recursos hoy pueden alcanzar objetivos en la red, situación que en otras circunstancias no era posible. Dicho de otra manera, los potenciales atacantes pueden ser muy inferiores al atacado, en relación a medios técnicos, pero con pocos medios pueden crear un virus con potencial maligno que cause gran impacto en forma anónima y clandestina, afectando a la seguridad nacional de los estados. (Pérez, 2018).

Para entender la seguridad y defensa desde el contexto del ciberespacio se debe tomar en cuenta dos palabras que podrían confundirse con facilidad: la Ciberseguridad y la Ciberdefensa; la primera de ellas es mucho más amplia, abarca varios ámbitos del Estado y la segunda debe entendérsela como una responsabilidad propia asignada a las Fuerzas Armadas (Fuertes, 2017)

Cuando se habla de Ciberseguridad, se refiere al "conjunto de acciones de carácter preventivo que tienen por objeto el asegurar el uso de las redes propias y negarlo a terceros" y más ampliamente se dice que "conjunto de herramientas, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión de riesgos, acciones, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse para proteger los activos

de la organización y los usuarios en el ciberentorno". Los activos de la organización y los usuarios son los dispositivos informáticos conectados, los usuarios, los servicios, aplicaciones, los sistemas de comunicaciones, las comunicaciones multimedios y la totalidad de la información transmitida y/o almacenada en el ciberentorno.[29]

La Ciberdefensa se conceptúa como "El conjunto de acciones de defensa activas, pasivas, proactivas, preventivas y reactivas para asegurar el uso propio del ciberespacio y negarlo al enemigo o a otras inteligencias en oposición"; o como también como lo detalla Francisco Zea al decir que "Es el conjunto de recursos, actividades, tácticas, técnicas y procedimientos para preservar la seguridad de los sistemas de mando y control, la información que maneja, y garantizar el libre acceso al ciberespacio de interés militar y permitir el desarrollo eficaz de las operaciones militares y el uso eficiente de los recursos" (citado en Fuertes, 2017).

El accionar de cibercriminales comunes y Ciberterroristas en el ciberespacio es una preocupación permanente para la defensa de los estados, quienes actualmente se preparan en términos estratégicos para enfrentar esta amenaza que en el ciberespacio presenta frecuentemente las características de un conflicto asimétrico anónimo y clandestino.

El termino ciberguerra, se refiere al desplazamiento de un conflicto, en principio de carácter bélico, que toma el ciberespacio y las tecnologías de la

[29] Información del COCIBER

información como escenario principal en lugar de los campos de batalla convencionales en el cual se busca alterar la información y los sistemas del oponente, a la vez que se protegen los propios (Badillo, 2017)

La ciberguerra ha evolucionado desde la dimensión militar al sector privado o comercial; este desarrollo representa una gran amenaza, hoy en internet podemos encontrar y descargar ciberarmas que las pueden dirigir en contra de sistemas civiles, económicos, financieros o infraestructuras críticas del Estado a un precio irrisorio. (Pérez, 2018)

En el caso de una eventual “ciberguerra” se pueden provocar daños que exceden las posibilidades de la mayoría de las armas convencionales por ejemplo la posibilidad de colapsar e incluso dañar físicamente los sistemas financieros como los sistemas bancarios, las redes globales de comunicación, sistemas de transporte como la regulación del tráfico aéreo y terrestre, sistemas industriales, control de infraestructuras críticas de abastecimiento energético y de agua, sistemas militares como radares etc., no solo les confiere letalidad, sino también la capacidad de provocar una alteración social y económica de consecuencias imprevisibles (Clarke, 2017)

De acuerdo a (Soriano, 2017), se calcula que entre veinte y treinta países han creado dentro de sus Fuerzas Armadas unidades especializadas en ciberguerra. Mencionadas unidades tienen como misión fundamental desarrollar las capacidades necesarias para combatir en una nueva dimensión del conflicto bélico, permitiéndoles garantizar la seguridad cibernética y la capacidad de

respuesta inmediata en caso de incidentes en el ciberespacio. Bajo ese contexto, la modernización de las Fuerzas Armadas Ecuatorianas, se basa en varios ejes estratégicos que entre otros incluye nuevas capacidades operativas como la Ciberdefensa.

Una eficaz reacción para proteger la información y la infraestructura crítica de un país debe sustentarse en una planificación estratégica, basada en las capacidades para desarrollar una conciencia situacional del nuevo teatro de operaciones, la naturaleza de las amenazas y la doctrina de empleo de los medios.

Las capacidades estratégicas para la Ciberdefensa deben desarrollarse y enfocarse en la detección y geo referencia de las amenazas cibernéticas, el análisis y la gestión del riesgo de la Ciberseguridad, la valoración permanente de las vulnerabilidades y debilidades de los sistemas telemáticos, garantizar la continuidad y disponibilidad de los sistemas de información e infraestructuras críticas de un estado nación; el desarrollo de ciberarmas y habilidad para explotar los nuevos avances tecnológicos de los sistemas de telecomunicaciones y redes informáticas (Fuertes, 2017)

Tipo de Investigación.

Para realizar este Proyecto se utilizó un tipo de investigación:

- Investigación de Campo

La investigación de campo es aquella que consiste en la recolección de

datos directamente de los sujetos investigados, o de la realidad donde ocurren los hechos (datos primarios), sin manipular o controlar variables algunas, es decir, el investigador obtiene la información, pero no altera las condiciones existentes. De allí su carácter de investigación no experimental.

Claro está, en una investigación de campo también se emplea datos secundarios, sobre todo, los provenientes de fuentes bibliográficas, a partir de los cuales se elabora el marco teórico. No obstante, son los datos primarios obtenidos a través del diseño de campo, lo esenciales para el logro de los objetivos y la solución del problema planteado.[30]

Población.

El universo de la presente investigación va estar orientado ha obtener información del personal de oficiales que actualmente se encuentran realizando el curso de Estado Mayor con la finalidad de ser comandantes, considerando que este personal de oficiales va estar involucrado directamente en las diferentes operaciones en las unidades militares que sean dados el pase.

Si la población es finita, se conoce el total de la población y se desea saber cuántos del total se tendrá que estudiar la fórmula sería: (Castellanos, 2018)

$$\mathrm{n} = \frac{\mathrm{K}^{\wedge 2} * \mathrm{p} * \mathrm{q} * \mathrm{N}}{\left(e^{\wedge 2} * (\mathrm{N} - 1)\right) + K^{\wedge 2} * \mathrm{p} * \mathrm{q}}$$

[30] Fidias G. Arias (2018)

Dónde:

N = Total de la población = 131,

k= 1.65 al cuadrado (si la seguridad es del 90%)

e= proporción esperada (en este caso 5% = 0.5)

q = 1 – p (en este caso 1-0.5 = 0.5)

p (en este caso 1-0.5 = 0.5)

N= 89

Se obtuvo una muestra de 89 oficiales para la aplicación de instrumentos de recolección de datos[31].

Muestra.

La muestra de la presente investigación es el personal que labora en el Comando de Ciberdefensa. Que se creó en cumplimiento al acuerdo ministerial 281 que en sus considerandos indica: “que, es necesario que en el nivel del CC.FF.AA. AA. Se Cree una instancia que implemente las directrices del nivel político, así como la capacidad de Ciberdefensa”.

Y en cumplimiento del art. 7. El COCIBER, se conforma como un comando del CC.FF.AA., integrado por personal técnico y operativo civil y militar. Tendrá la misión de operar las capacidades de defensa, explotación y respuesta en el espacio cibernético, para proteger y defender la infraestructura crítica e información estratégica del estado.”

[31] Feedback Networks.com

Métodos de Investigación.

Esta investigación se la realizará mediante el método de investigación científica básica.

También se utilizará una investigación explicativa o de comprobación de hipótesis causales, por cuanto se parte de una situación problema o conocimiento presente para luego indagar posibles causas o factores asociados que permiten interpretarla.

Técnicas de Recolección de datos.

El método que se empleará en la investigación es la encuesta y la observación con la modalidad de cuestionarios, que serán aplicadas a Oficiales del CEMA N.º 70[32] y al personal involucrado en el desarrollo de los proyectos de Ciberdefensa, las consecuencias a la seguridad ecuatoriana, ocasionada por las amenazas latentes en el país, ya que ellos son los que conocen de cerca este problema, ya que han estado dirigiendo directamente las operaciones realizadas por sus diferentes unidades operativas, de allí se obtendrán datos importantes que servirán para cuantificar y medir las interrogantes sobre las variables objeto de investigación.

Instrumentos de Recolección de datos.

El instrumento que se utilizará será la entrevista dirigida a expertos y encuestas, la información que se pueda encontrar en base a su acceso y se lo dividirá en fuentes primarias y secundarias, basadas en un estudio del arte y sus

[32] CEMA 70: Curso de Estado Mayor de Arma

tendencias inicialmente, y servirá para conocer la situación actual en el desarrollo de las capacidades del Comando de Ciberdefensa ya que estas contribuyen a la capacidad de Comando y control que tiene que desarrollar las Fuerzas Armadas ante las amenazas y riesgos existentes en el País.

Los estudios prospectivos y su recolección analizan la situación actual a partir de sucesos acontecidos en el pasado. “Los estudios prospectivos se inician con la observación de ciertas causas presumibles y avanzan longitudinalmente en el tiempo a fin de observar sus consecuencias”[33]. Esta investigación posee una característica fundamental, es la de iniciarse con la exposición de una supuesta causa, y luego seguir a través del tiempo a una población determinada hasta determinar o no la aparición del efecto.

Las encuestas se realizarán a través de la web en Google (Anexo “A”) y se las realizará a personal de alumnos del CEMA 70, así como también al personal que haya estado involucrado en el desarrollo de los proyectos de Ciberdefensa, todo esto para ampliar el conocimiento del desarrollo de los proyectos que se encaminan a satisfacer las necesidades existentes.

Para realizar la recolección de información de fuentes secundarias se hará énfasis en el análisis documental y la revisión y lectura de informes, estudios anteriores, manuales normativos y publicaciones inherentes al tema.

[33] Procedimientos y técnicas de recogida de información para la investigación educativa, Marta Alelú Hernandez,2018

Técnicas para el análisis e interpretación de Datos.

Este conjunto de técnicas estadísticas emplea datos de series temporales para predecir cuál es el resultado más probable que se puede dar en el futuro cercano. La base de estas técnicas de análisis de datos es fijarse en que es lo que ha ocurrido en el pasado para saber qué ocurrirá en el futuro.

La fase de análisis e interpretación de resultados tiene que ver con las operaciones matemáticas a las cuales se someten los datos con la finalidad de comprobar las Hipótesis propuestas en esta investigación, por lo que nos ayudaremos con los estadígrafos descriptivos, los mismos que se ocupan de analizar los datos, valores o puntuaciones de la o las variables en estudio de forma separada, el tipo de prueba estadística dependerá del nivel de medición que se tenga entre los más importantes que se disponen son los porcentajes, proporciones, razones, tasas, media aritmética, medina, moda y desviación estándar.

Análisis De Resultados De La Entrevista Y Encuesta.

Aplicación de la entrevista

Las preguntas de la entrevista, fueron divididas en dos partes, la primera parte inicial es para verificar las actividades que se ejecutan dentro de la Sección de Capacidades y la segunda parte es para entender sobre cómo fue concebido la planificación de capacidades en la Fuerza Terrestre.

La entrevista fue realizada a las 14:00 horas del día martes 26 de marzo del 2019 en el despacho de Sr. Tcrn. E.M. Narváez Mauricio, encargado

de lo que son capacidades de la Fuerza Terrestre, la misma que se transcribe a continuación:

Entrevista

1. **¿Cómo están estructuradas las capacidades en la Fuerza Terrestre?**

La capacidad de la Fuerza Terrestre se despliega en base de la capacidad de maniobra, la que constituye la base para que se desplieguen las seis capacidades que actualmente tiene la Fuerza.

Actualmente en la Fuerza se han desplegado las capacidades de: infantería, operaciones en selva, operaciones aeroterrestres, operaciones especiales, apoyo de juego y apoyo de ingeniería. Las comunicaciones son a través del mando y control, que se ha venido desarrollando en base a: seguridad de los sistemas de información y guerra electrónica.

La última capacidad que se incorporó es la de gestión de riesgos la misma que fue colocado por una situación institucional y en consenso de todas las fuerzas se logró para mayor accesibilidad en lo que es equipo y medios. Para poder cuantificar la capacidad que tiene un determinado sistema, se calcula a través de la operatividad y operabilidad. Operatividad lo que se refiere a recursos humanos y la operabilidad a recursos y medios.

2. **¿Cuál fue el proceso que definió las seis áreas de capacidades que ahora tiene la Fuerza Terrestre?**

Las áreas de capacidades que actualmente tiene la fuerza son aquellas que se determinó para cumplir con todas las operaciones terrestres en cumplimiento a las misiones asignadas. Las misiones que se requiere cumplir están inmersas en el árbol de capacidades; además está relacionado con el escenario operacional que cada una de las jurisdicciones militares tiene, en base al escenario operacional que estableció el Comando Conjunto el cual es un escenario prospectivo, en base a ese escenario la Fuerza hizo su escenario y en base a este escenario con un mayor análisis se determinó las amenazas y riesgos que se va afrontar; todo esto sirvió para de acuerdo al escenario que se iba afrontar fortalecer la capacidad de acuerdo a cada jurisdicción, estos escenarios están materializados en el Plan de Capacidades 2016.

3. **¿Considera que podría existir algún problema cuando las Capacidades del Comando Conjunto estiman seis componentes para determinar las capacidades mientras que la Fuerza solo tiene cuatro componentes?**

Hay que indicar que el desarrollo de capacidades lo tiene más adelantado la Fuerza Terrestre, ya que a partir del 2010 se comenzó a

desarrollar esta planificación. El manual que actualmente se tiene es una propuesta, todavía no está aprobado, en el que se ha venido discutiendo analizando, pero si analizamos en la fuerza se tiene: recurso humano, infraestructura, la doctrina que actualmente fue traída de España y es la que mayoría de países lo han adoptado, la misma que se alinea a ciertas directrices de la OTAN para poder tener una fuerza con ciertas capacidades especiales para que desplegarse a misiones por todos países. LA OTAN pide unidades militares con estas capacidades, no un batallón de infantería, batallón de artillería, por lo que ellos si debe mediar la organización, para nosotros en cambio la organización ya están establecido. El diseño de fuerza nace a través de unos escenarios, a esos escenarios el sector político debe decirnos que la Fuerza Terrestre debe hacer, frentes a esos escenarios debemos cumplir misiones y tareas, así como otras instituciones del estado para hacer frente a ese escenario operacional mediante misiones y tareas. Teniendo ya presente las misiones y tareas que debe cumplir las Fuerzas Armadas, por lo que buscamos esas capacidades para cumplir las misiones. Obtenido las capacidades determinamos la estructura que debe tener la Fuerza Terrestre a eso se complementa con la asignación de personal y se determina requerimientos operacionales.

Por lo que se puede decir que, si hubiéramos cumplido toda la planificación, se puede afirmar que el ultimo orgánico 2017-2021 obedeció a un diseño que fue impuesto por el poder político, esto se

trabajó aisladamente sin que las demás fuerzas y por eso es el motivo que no esta tan alineado a lo que tiene el CC.FF.AA.

Pero ya tenemos una estructura por eso no se tiene la organización, además que no existe un criterio para medir la organización.

4. **¿Cómo fue implantado el sistema para medir las capacidades de la Fuerza Terrestre y no sé si es similar a lo que aplican en España?**

Se puede indicar que de España se sacó la doctrina de lo que planificación por capacidades, pero allá no se encuentra implementado un software para medir capacidades. En Ecuador se creó este software considerando las particularidades de nuestra Fuerza con la finalidad de saber si podemos hacer frente esa diversidad de escenarios y en base a este identificar los requerimientos operacionales que se pretende informar.

5. **¿Cómo se mide las capacidades de la Fuerza Terrestre?**

Se mide a través de los componentes personal, material, infraestructura y doctrina, con esto se mide las Sub-capacidades que debe tener una capacidad para poder cumplir su misión específica que viene por cada una de las armas estas matrices ya existen deben ser

revisadas, para evaluar esa matriz si está realmente aborda todas las capacidades que debe tener un sistema.

6. **¿Las capacidades actuales en base a qué criterios lo determinaron?**

El sistema permite ver como se determina las capacidades, para finalmente consolidar en base a una misión general y misiones específicas que deben cumplir con esto se determina cual es la capacidad que debe tener para esta capacidad se necesita las capacidades especificas o Sub-capacidades y condición que se encuentra y esto se hace a través de los componentes, personal en base al orgánico, entrenamiento, equipo y medios en base a las tablas de organización y equipo.

7. **¿Cómo actualmente se traducen los niveles de las capacidades?**

Se ha trabajo bastante en base a proyectos en cada uno de los campos que necesita de todos los sistemas. Se ha determinado áreas críticas para cada uno de los sistemas, esto es lo mínimo que debería tener el Ejército, así se hayan concebido sistemas más modernos conforme las nuevas tecnologías como por ejemplo una infantería más liviana, complementado esto con la investigación y desarrollo.

El sistema le da por campos, defensa externa, ámbito interno y gestión de riesgo, los resultados están disminuidos para defensa externa material y equipo, defensa interna se cambia totalmente la matriz se adapta para cada una de las áreas y el sistema le arroja el valor, las unidades llenan las matrices, que van desde compañía independientes, batallones, brigadas y divisiones. Los valores casi se mantienen, aportan los proyectos de mantenimiento, así esta operacionalizado toda la teoría por capacidades, se llega a un consolidado el resumen con un porcentaje con todas sus unidades como Estado Mayor, Comando Apoyo Logístico.

Análisis de la entrevista

A continuación, se detalla las principales conclusiones de las respuestas dadas por el entrevistado:

- Las capacidades que se han desarrollado en la Fuerza Terrestre tienen como fundamento doctrinario lo que las Fuerzas Armadas de España han realizado, doctrina que se ha ido acoplando a nuestra realidad, especialmente en lo que comprende los componentes que definen una capacidad, además de haberse implantado un software que permite obtener valores porcentuales de las capacidades de cada uno de los sistemas.

- Las capacidades que actualmente se han desarrollado están en directa relación con el escenario operacional en el cual van actuar

las unidades para cumplir sus misiones de defensa externa, ámbito interno y gestión de riesgos.

- Para recuperación de cada una de las capacidades se han considerado proyectos, los mismos que están en espera de que sean aprobados para que entren en ejecución y disminuya la brecha operacional que actualmente existe.

- La línea base que toma el software para medir las capacidades son los aspectos de operatividad y operabilidad, que están en función de los orgánicos de las unidades, las tablas de organización y equipo y rendimiento de pruebas físicas.

- La planificación por capacidades se inicia en la Fuerza Terrestre y posteriormente el Comando Conjunto toma esta planificación para definir las capacidades del Comando Conjunto.

Tabulación de datos de las encuestas.

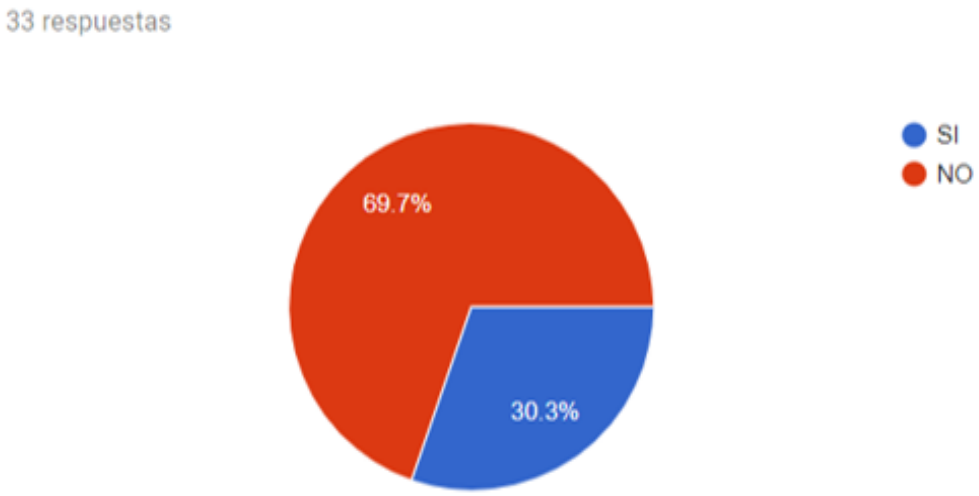
A continuación, se presentan los resultados, procesados y analizados, producto de la investigación que sirvieron para identificar las capacidades específicas y los posibles componentes para la matriz de capacidad operativa del COCIBER.

Pregunta Nº 1

¿Conoce usted la misión que cumple el Comando de Ciberdefensa (COCIBER) del Comando Conjunto de las Fuerzas Armadas?

Figura 1

Porcentaje de la misión que cumple el COCIBER



Nota: Tabulación de respuestas a encuestas en www.docs.google.com/forms.

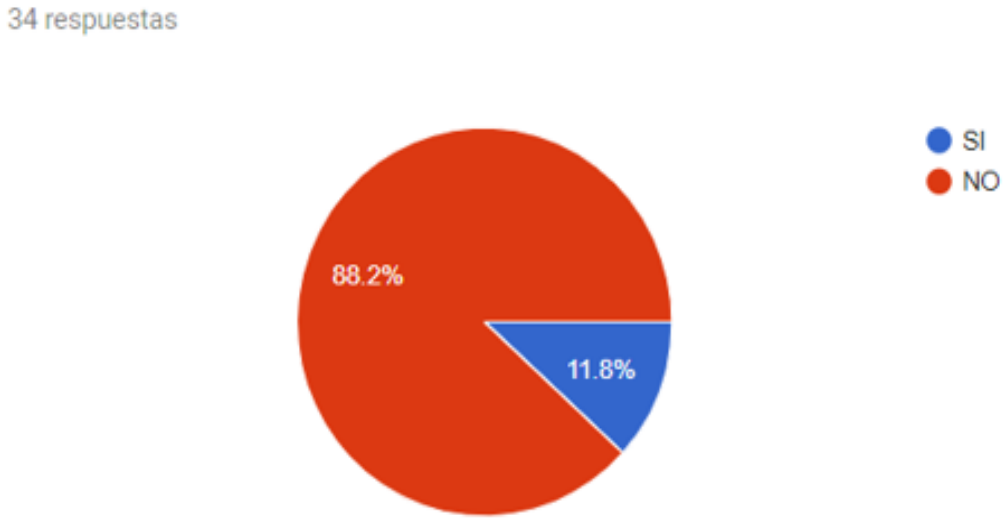
Analizando esta pregunta nos podemos dar cuenta que un porcentaje alto de 23 encuestados que representan el 69,7% manifestaron que no conocen la misión que cumple el Comando de Ciberdefensa del Comando Conjunto de Fuerzas Armadas; mientras que un mínimo porcentaje de 10 encuestados que representan el 30,3% indican que si conocen la misión que cumple el Comando de Ciberdefensa.

Pregunta Nº 2

¿Conoce usted cuales son las capacidades del Comando de Ciberdefensa?

Figura 2

Porcentaje de las capacidades del COCIBER



Nota: Tabulación de respuestas a encuestas en www.docs.google.com/forms

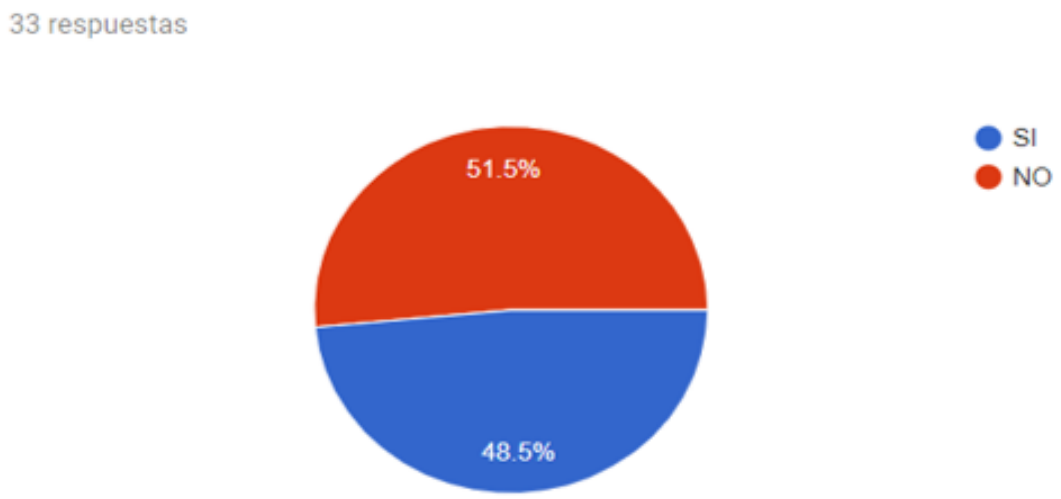
Analizando esta pregunta nos podemos dar cuenta que un porcentaje alto de 29 encuestados que representan el 87,9% manifestaron que no conocen las capacidades del COCIBER del CC.FF.AA; mientras que se evidencia un mínimo porcentaje de 5 encuestados los mismos que representan el 12,1% e indican que si conocen las capacidades que cumple el Comando de Ciberdefensa.

Pregunta Nº 3

¿Conoce usted cuales son las amenazas y riesgos de la Ciberdefensa?

Figura 3

Porcentajes de las amenazas y riesgos de la Ciberdefensa



Nota: Tabulación de respuestas a encuestas en www.docs.google.com/forms

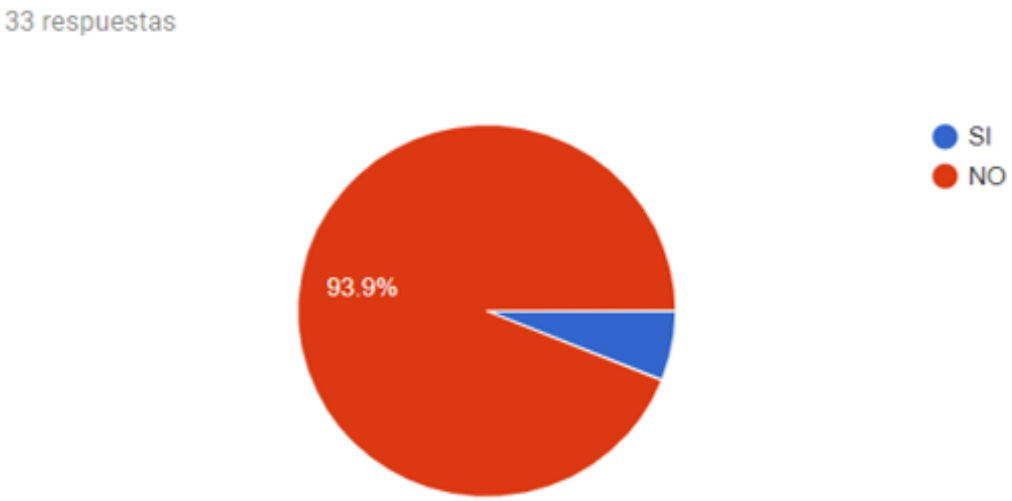
Analizando esta pregunta nos podemos dar cuenta que existe un porcentaje casi parejo vista 17 encuestados que representan el 51,5% manifestaron que no conocen las amenazas y riesgos de la Ciberdefensa; mientras que se evidencia un similar porcentaje de 16 encuestados que representan el 48,5% los mismos indican que si conocen la amenazas y riesgos.

Pregunta Nº 4

¿Conoce usted si el COCIBER dispone de una matriz que permita determinar el porcentaje al que se encuentra su capacidad operativa?

Figura 4

Porcentaje de la capacidad operativa del comando de Ciberdefensa



Nota: Tabulación de respuestas a encuestas en www.docs.google.com/forms

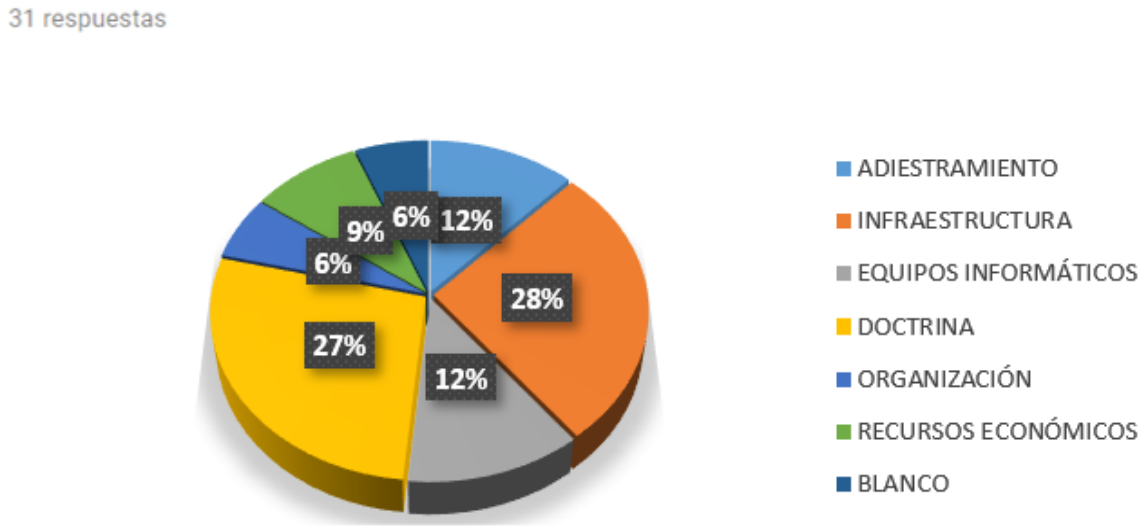
Analizando esta pregunta nos podemos dar cuenta que existe un porcentaje demasiado alto de 31 encuestados que representan el 93,9%, mismos que manifestaron que no conocen si el COCIBER dispone de una matriz que permita determinar el porcentaje al que se encuentra su capacidad operativa; mientras que se evidencia un mínimo porcentaje de 2 encuestados que representan el 6,1%, los mismos que indican que si conocen.

Pregunta Nº 5

¿De acuerdo a la respuesta de la pregunta anterior, indique que aspectos tiene o que componentes se debería considerar en la matriz capacidad operativa?

Figura 5

Porcentaje de la capacidad operativa del comando de Ciberdefensa



Nota: Tabulación de respuestas a encuestas en www.docs.google.com/forms

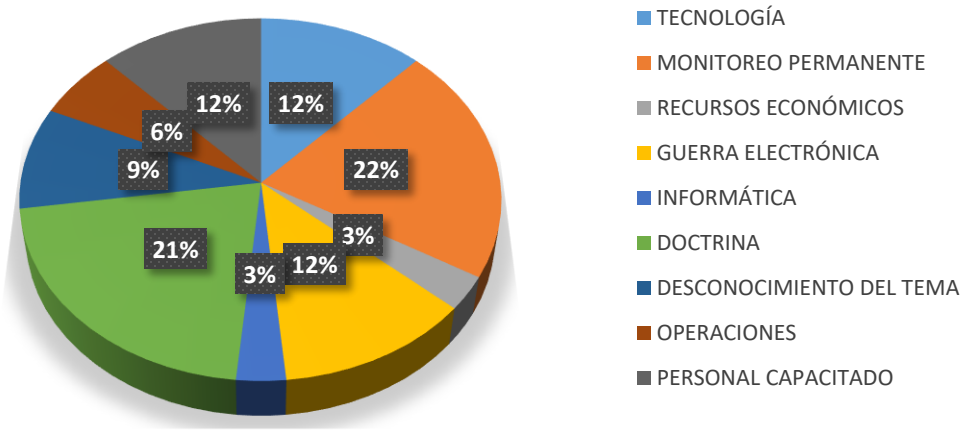
Analizando esta pregunta nos podemos dar cuenta que existe un porcentaje mínimo de acuerdo a la mayoría de los encuestados, y se puede evidenciar que están de acuerdo con los parámetros que se han considerado para una matriz de capacidad operativa del COCIBER y se evidencia únicamente dos encuestados que indica que debería haber otro aspecto a considerar en la matriz de capacidad operativa.

Pregunta Nº 6

¿De acuerdo a la respuesta de la pregunta anterior, indique que componentes adicionales considera que debería tener la matriz capacidad operativa del COCIBER?

Figura 6

Porcentaje de componentes adicionales en matriz de capacidad operativa del Comando de Ciberdefensa



Nota: Tabulación de respuestas a encuestas en www.docs.google.com/forms

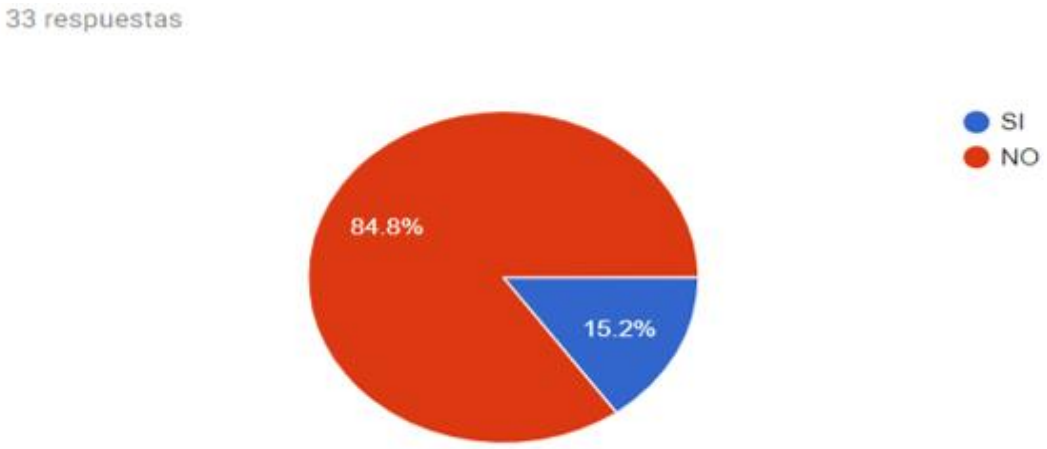
Analizando esta pregunta nos podemos dar cuenta que existe un porcentaje mínimo de acuerdo a los encuestados indican que los siguientes componentes adicionales debería tener la matriz de capacidad operativa del COCIBER: guerra electrónica, informática, monitoreo permanente, operaciones, tecnología, personal capacitado y con valores y recursos económicos. Cabe señal que muchos indican que desconocen del tema.

Pregunta Nº 7

¿Conoce usted si existen proyectos relacionados a fortalecer el COCIBER?

Figura 7

Porcentajes de proyectos a fortalecer el Comando de Ciberdefensa



Nota: Tabulación de respuestas a encuestas en www.docs.google.com/forms

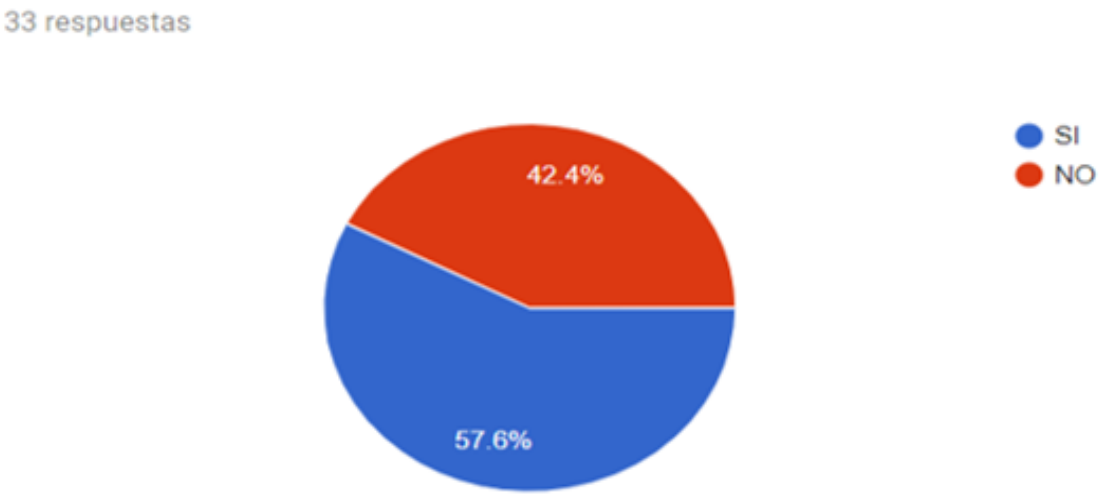
Analizando esta pregunta nos podemos dar cuenta que existe un porcentaje mínimo de 28 encuestados que representan el 84,8%, los mismos que manifestaron que no conocen si existen proyectos relacionados a fortalecer el Comando de Ciberdefensa; mientras que se evidencia un mínimo porcentaje de 5 encuestados que representan el 15,2%, los que indican que si conocen proyectos relacionados a fortalecer el COCIBER.

Pregunta Nº 8

¿Conoce usted que debería haber cursos o seminarios de capacitación sobre Ciberdefensa?

Figura 8

Porcentajes de proyectos a fortalecer el Comando de Ciberdefensa



Nota: Tabulación de respuestas a encuestas en www.docs.google.com/forms

Analizando esta pregunta nos podemos dar cuenta que existe un porcentaje mínimo de 19 encuestados que representan el 57,6%, los mismos que manifestaron que si debería haber cursos o seminarios de capacitación sobre Ciberdefensa; mientras que se evidencia un mínimo porcentaje de 14 encuestados que representan el 42,4%, indican que no debería haber cursos o seminarios.

ANÁLISIS GENERAL DE LA ENCUESTA

Tabla 1

Tabulación de respuestas a encuestas en www.docs.google.com/forms

CUADRO RESUMEN DE TABULACIÓN DE ENCUESTA		
PREGUNTA	**SI**	**NO**
1	10	23
2	4	29
3	16	17
4	2	31
5	mayoría	minoría
6	Capacidades adicionales.	Desconocen
7	5	28
8	19	14

Capítulo IV

DESARROLLO DE LOS OBJETIVOS.

Primer Objetivo Específico y/o Tarea Científica

Analizar el escenario prospectivo de Fuerzas Armadas en el campo de la Ciberdefensa.

Introducción

Actualmente el Comando Conjunto de las Fuerzas Armadas se encuentra frente a un entorno complejo, incierto y dinámico y es justamente en esa incertidumbre cuando funciona la prospectiva la cual ha sido empleada por gobiernos de varios países. En la actualidad, ya no es posible realizar solo el planeamiento estratégico tradicional, ni en lo político, ni en lo empresarial, ni en lo militar, basados en una “visión” única y siempre deseable para las instituciones; sino que es preciso contar con estrategias claras, además de planes de contingencia basados en diferentes escenarios alternativos, posibles y probables, es aquí donde la prospectiva produce su mayor beneficio.

Conocimiento del Hecho

En el ámbito internacional se han producido cambios en la estructura geopolítico-mundial, con tendencias a la globalización y la fragmentación de

los estados-nación; han aparecido nuevos espacios geopolíticos y nuevas alianzas estratégicas, la conformación de espacios económicos regionales y extensas regiones marginales.

Los conflictos armados entre los Estados son menos probables; sin embargo, el mundo se ha tornado más impredecible, inestable, ambiguo y complejo; en la actualidad y en el futuro los conflictos internos con repercusiones regionales, son más frecuentes, lo que privilegia la atención a la cooperación interestatal, interinstitucional e interagencial, permitiendo a los Estados mejorar su capacidad de lucha contra las nuevas amenazas, especialmente aquellas relacionadas con: los grupos ilegales armados, la inseguridad ciudadana, el tráfico de drogas, la trata de personas, el crimen organizado transnacional, la piratería marítima, la contaminación ambiental, el cambio climático y los desastres naturales[34].

Asimismo, la constante amenaza ciberespacial, con la posibilidad de colapsar e incluso dañar físicamente los sistemas de información a lo que se suman: el espionaje, sabotaje y el rastreo cibernético, ejecutados no sólo por *hackers, crackers, script bunnies, insiders* informáticos, sino de: terroristas, organizaciones criminales y extremistas políticos, movimientos sociales, religiosos, servicios de inteligencia y fuerzas militares extranjeras.

Al interior de la institución se ha completado la reestructuración de Fuerzas Armadas, proceso que ha permitido un dimensionamiento de fuerza

[34] Plan de Gestión Institucional de FF. AA 2010 - 2021

acorde al nuevo escenario estratégico, implementando una organización dinámica y flexible, que facilita cumplir las misiones de las Fuerzas Armadas mediante la integración sinérgica y coordinación de los organismos de planificación, preparación, empleo y apoyo de manera efectiva; se ha consolidado el sistema de inteligencia militar, el sistema de salud y de seguridad integral, también se ha alcanzado la reubicación y conformación de unidades en fuertes o bases militares, se evidencia una organización con modelos de concentración regional, unidades orgánicamente completas, de cuadros profesionales, interoperables, flexibles con capacidad de despliegue rápido y empleo conjunto en cualquier parte del territorio nacional, debidamente dotadas y tecnológicamente bien equipadas, en todos sus sistemas operativos, y en condiciones de enfrentar los nuevos desafíos tales como: los problemas derivados de la inseguridad, la afectación psicosocial, el deterioro al ambiente y la constante amenaza ciberespacial.[35]

Análisis

Los problemas de límites, los históricos pendientes, la lucha por recursos vitales, las reivindicaciones de tipo religioso, diferencias étnicas, de género, la globalización del comercio entre otros motivos, han generado conflictos entre actores estatales y no estatales, una de las alternativas de solución a sus disputas en los dominios de la tierra, el mar y el aire fue y es

[35] Plan de Gestión Institucional de FF.AA 2010-2021

aún el uso del poder terrestre, naval y aéreo, conforme los alcanzaban evolutivamente.

Es evidente que en el siglo anterior los avances en las técnicas de la información y de las comunicaciones se reflejan en ingenios usados en el cuarto dominio denominado espacial y con mayor impacto en el quinto dominio el ciberespacio, el mismo que además de pulverizar las barreras de tiempo y distancia obligo a establecer nuevos esquemas de defensa a las Fuerzas y Cuerpos de Seguridad para enfrentar los nuevos desafíos del siglo XXI en un teatro de operaciones virtual. En el ciberespacio se desarrollan dos tipos de operaciones: las de Ciberseguridad orientadas a minimizar el nivel de riesgo al que están expuestos los ciudadanos ante amenazas de índole cibernético y las de Ciberdefensa encaminadas a garantizar el sentido de seguridad del Estado Nacional.

Estas estrategias impulsan a que el sector de la Defensa y Fuerzas Armadas como órgano operativo, coadyuven al Estado ecuatoriano en el desarrollo de la capacidad de Ciberdefensa, a través de un conjunto de medidas y gestiones destinadas a alcanzar las condiciones de seguridad en el ciberespacio. Para hacer frente a los nuevos requerimientos es necesario incrementar capacidades específicas en función de cuatro componentes fundamentales: Estructura organizacional, Procesos probados, Personal altamente entrenado y Tecnología de vanguardia, orientados a iniciar el desarrollo de una adecuada capacidad estratégica conjunta de Ciberdefensa

para mitigar o anular el interés sobre blancos civiles y militares propios de posibles adversarios o potenciales enemigos

Conclusiones Parciales

La participación en la seguridad integral, por parte de Fuerzas Armadas, conlleva la tarea de realizar operaciones de protección a las áreas de infraestructura estratégica a nivel del territorio continental, marítimo, insular, aéreo y cibernético cuya criticidad depende del impacto que puede ocasionar la interrupción o destrucción de las instalaciones asociadas a las infraestructuras críticas tales como redes eléctricas y de telecomunicaciones, servicios que afecten las actividades económicas, productivas, laborables, la gobernabilidad y los derechos y deberes de los ciudadanos.

La gran dinámica del desarrollo nacional, se ha traducido, por una parte en el fortalecimiento de la automatización e interconexión de redes, de procesos de sistemas de control del tráfico terrestre, marítimo y aéreo, de la generación eléctrica, del sistema de agua potable, del sistema de salud, de las rentas internas, del área financiera, de compras públicas, entre otros. También la dinámica nacional se manifiesta en el fortalecimiento de las FF.AA., en sus sistemas operativos de aplicaciones informáticas para Inteligencia, Operaciones, Personal, Logística, Abastecimientos, Sanidad, Finanzas, Presupuesto, entre otros.

Pero por otra parte esa dinámica nacional y mundial ha creado y dejado expuestas muchas vulnerabilidades en el ciberespacio de la sociedad

en su conjunto. La protección y defensa de los recursos e información estratégica de las FF.AA; y del Estado deben responder a un concepto integral de defensa física y virtual, quedando lejos el concepto operacional de emplear exclusivamente equipos cinéticos y guardias bien entrenados para proteger la infraestructura crítica controlada por las TIC's. Los nuevos retos que plantean el ciberespacio y en particular la Ciberdefensa, Fuerzas Armadas sabrán afrontar de forma decidida, en armonía con el apoyo de toda la ciudadanía.

Segundo Objetivo Específico y/o Tarea Científica

Analizar los aspectos doctrinarios que deber ser tomados en consideración para el desarrollo de las capacidades del ciberespacio.

Introducción

La doctrinaria que se plantea es en base a las operaciones de Ciberdefensa de las Fuerzas Armadas de Estados Unidos, la cual busca definir aquellos aspectos que deben ser tomados en consideración para el desarrollo de las capacidades del ciberespacio y para la planificación y ejecución de las operaciones en el ciberespacio por parte del Comando de Ciberdefensa del Comando Conjunto de las FF.AA., en apoyo a las otras operaciones militares que se planifican y ejecutan por parte de una fuerza conjunta, en una Zona/ Teatro de Operaciones Conjunto, para la consecución de los objetivos asignados.

Los aspectos contenidos en este documento, pueden constituirse en una guía para el Comando de Ciberdefensa, para que, de manera integrada y coordinada por el Estado Mayor del Comando Conjunto, permitan al Comandante de la Fuerza Conjunta, CFC[36] y sus comandantes operativos, la integración de los aspectos inherentes a las Operaciones en el Ciberespacio, con la planificación para el cumplimiento de los requerimientos, tareas y misiones contempladas en su plan de operaciones.

Conocimiento del Hecho

El Ministerio de Defensa Nacional velará por el fortalecimiento de las capacidades operativas pertinentes y desarrollará las políticas específicas en el ámbito aeroespacial, Ciberdefensa, gestión de riesgos, seguridad integral, empleo progresivo de la fuerza contra vuelos ilegales y misiones de inteligencia.[37]

Esta publicación, se enfoca en las operaciones militares que se desarrollan en o dentro el Ciberespacio; explican el relacionamiento y las responsabilidades del Estado Mayor Conjunto, de los Comandantes Operacionales, del Comando de Ciberdefensa (G-6), de las fuerzas, y de las unidades o agencias de apoyo de combate; y, establece la estructura para el empleo de las fuerzas y capacidades en el Ciberespacio.

[36] Comandante de la Fuerza Conjunta, CFC
[37] Agenda Política de la Defensa 2014 - 2017

El Ciberespacio que es parte del ambiente de la información, depende de los dominios físicos del aire, tierra, marítimo y espacial. Las OC emplean links y nodos localizados en los dominios físicos y ejecutan funciones lógicas para crear efectos primeramente en el Ciberespacio y luego, de ser necesario, en los dominios físicos. Las acciones en el Ciberespacio, desarrolladas mediante un cuidadoso y controlado efecto de cascada, pueden garantizar la libertad de acción del comandante, para las actividades en los dominios físicos.

Todas las acciones que se desarrollan en el ciberespacio son actividades que puedan ser relacionadas como parte de las tres misiones en el ciberespacio: operaciones ofensivas en el ciberespacio (OOC), operaciones defensivas en el ciberespacio (ODC) o las operaciones del Comando Conjunto en el ciberespacio. Estas tres misiones cubren totalmente las actividades de las fuerzas del ciberespacio. La ejecución exitosa de las OC, requiere de la integración y sincronización de estas tres misiones.

Análisis

El Comando de Ciberdefensa del Comando Conjunto, busca cumplir su misión dentro de tres líneas de operaciones primarias: asegurar, operar y defender el Sistema de Información del Comando Conjunto(SICC), defender a las instalaciones estratégicas críticas de la nación de ataques cibernéticos y proporcionar apoyo cibernético a los Comandos Operacionales que lo requieran. Para ello dispone de personal y unidades entrenadas y equipadas para realizar OC.

El ciberespacio se extiende más allá de las fronteras físicas y geográficas, y está integrado con la operación de infraestructuras críticas, así como la conducción del comercio, el gobierno, y las actividades de la defensa nacional. La prosperidad y la seguridad de la nación están relacionadas estrechamente con el uso del ciberespacio, ya que su desarrollo incrementa la exposición a las vulnerabilidades y a la dependencia del ciberespacio de la nación en general y de las fuerzas armadas en particular.

Muchos aspectos de las operaciones conjuntas se basan en parte en la utilización del ciberespacio, dominio existente dentro del Ambiente Informacional (AI)[38], que consiste de la red interdependiente de la Tecnología de Información (TI)[39], infraestructura e información residente (base de datos). Incluye el internet, redes de telecomunicaciones, sistemas de computación, procesadores y controladores. Las Operaciones en el Ciberespacio (OC)[40], consisten en el empleo de las capacidades del ciberespacio, con el propósito primario de alcanzar objetivos en y mediante el ciberespacio.

La autoridad para la planificación ejecución de Operaciones militares en el ciberespacio está establecida dentro de las políticas emitidas por el Ministerio de Defensa, así como en las órdenes recibidas que autorizan al Comando de Ciberdefensa a la ejecución de estas operaciones.

[38] AI: Ambiente Informacional/ Área de Interés
[39] TI: Tecnología de Información
[40] OC: Operaciones en el Ciberespacio

Los responsables por la planificación y ejecución de las OC[41], deberán conocer y aplicar los principios y normas de empleo descritos en esta propuesta, que son de carácter general, producto de experiencias acumuladas por otras fuerzas armadas, y que, sumados a las experiencias propias, permitirán el desarrollo de las capacidades en el ciberespacio para la planificación y ejecución de las Operaciones en el Ciberespacio.

Conclusiones Parciales

Las OC comprenden las operaciones militares, nacionales y ordinarias que se desarrollan en el ciberespacio. Las operaciones militares en el ciberespacio están organizadas en misiones ejecutadas mediante una combinación de acciones específicas.

El ciberespacio es una actividad que sincroniza e integra la planificación y operación de los sensores; medios; y sistemas de procesamiento, explotación y diseminación, en apoyo a las operaciones decurrentes o futuras. Esta es una función de inteligencia integrada con las operaciones. La inteligencia, vigilancia y reconocimiento (IVR), en el ciberespacio se enfoca en la obtención de información táctica y operacional y en el mapeo de las redes del adversario para apoyar la planificación militar. Para facilitar la optimización de los todos los medios disponibles de IVR, un concepto de la operación de IVR debe ser desarrollado en conjunción con el esfuerzo de planificación del comandante.

[41] OC: Operaciones en el Ciberespacio

Cualquier usuario que no sigue cuidadosamente las políticas de ciber seguridad, puede constituirse en una amenaza interna. Actores maliciosos internos, pueden explotar su acceso en beneficio de gobiernos extranjeros, grupos terroristas, elementos criminales, asociados inescrupulosos, o en su propia iniciativa o beneficio. Ya sea que estos usuarios internos maliciosos estén realizando espionaje, realicen una declaración política, o expresen sus posturas personales, las consecuencias para el SICC y la seguridad nacional pueden ser desastrosas. El CFC debe utilizar medidas de mitigación para esta amenaza, como el reforzamiento del entrenamiento de la FC para estar alerta por actividades sospechosas internas y utilizar un control de dos personas sobre hardware, software o información sensible.

Tercer Objetivo Específico y/o Tarea Científica

Analizar la planificación por capacidades del Comando Conjunto de las FF.AA.

Introducción

La planificación basada en capacidades aplicada por las Fuerzas Armadas ecuatorianas, se sustentan en un conjunto de elementos que producen los efectos operacionales necesarios para cumplir las misiones asignadas y para enfrentarse a los retos futuros no se pueden improvisar. Es importante considerar que el diseño de fuerzas, el fortalecimiento de los sistemas de armas, la investigación tecnológica, el reclutamiento y formación de personal, y el alistamiento operacional, requieren tiempo de preparación,

todo ello bajo las exigencias de un entorno que se encuentra en continuo cambio.[42]

Las capacidades militares aplicada por Fuerzas Armadas, proporcionan un fundamento más racional para la toma de decisiones sobre la modernización del material existente, adquisiciones futuras y el sostenimiento operacional, a la vez que ofrece soluciones integrales, para afrontar con éxito los actuales y potenciales escenarios de conflicto. (Ardieta, 2013)

Conocimiento del Hecho

La Planificación de la defensa en nuestro país, nace del estudio de escenarios en función de las amenazas y riesgos de acuerdo al nivel de planificación, existiendo un vacío desde el nivel Político - Estratégico hacia el nivel de Estratégico – Militar. Es así que se afianza la planificación por capacidades de las Fuerzas Armadas, teniendo una relación lógica de los escenarios, capacidades, limitaciones, vulnerabilidades y necesidades para poder contar con una fuerza capaz de responder a cualquier amenaza y/o riesgo, en marcada de la política de Defensa actual.

El nuevo diseño de Fuerzas, debe responder al desarrollo de capacidades para el empleo conjunto de las Fuerzas Armadas, para enfrentar con éxitos las amenazas, riesgos y desafíos del Estado, en los actuales y futuros escenarios estratégicos de seguridad y defensa, así como en las amenazas emergentes. Por la experiencia vivida en 1995 y la incidencia del nuevo proceso de planificación a nivel mundial, a partir del año 2006 se inicia

[42] Plan de Gestión Institucional de FF.AA 2010-2021

el análisis y propuesta para implementar la planificación por capacidades a nivel Fuerzas Armadas.

El Sistema de Planeamiento por Capacidades determina las capacidades conjuntas y especificas respecto a los escenarios, amenazas, riesgos y misiones, su condición y requerimientos que permitan fortalecerlas evitando las necesidades y soluciones aisladas y no orientadas a la consecución de los objetivos propuestos.[43]

Análisis

La capacidad militar se define al conjunto de diversos factores (personal, sistemas de armas, infraestructura y medios de apoyo logístico) asentados sobre la base de principios doctrinales y procedimientos operativos, que pretenden conseguir un determinado efecto militar a nivel estratégico, operacional o táctico, en cumplimiento de las misiones asignadas, las capacidades que deben tener las Fuerzas Armadas ecuatorianas han sido determinadas por áreas de capacidades, capacidades, sub-capacidades, objetivos de capacidad militar y requerimientos operacionales los cuales les permitirán cumplir con las misiones asignadas.[44]

La determinación de las capacidades proporciona un fundamento más eficiente para la toma de decisiones sobre la modernización del material existente, adquisiciones futuras, adaptación y el sostenimiento operacional, a

[43] Sistema de Planeamiento por Capacidades del MIDENA 2016
[44] Sistema de Planeamiento por capacidades del MIDENA 2015

la vez ofrece soluciones integrales, para accionar con éxito en los actuales y potenciales escenarios.

La incertidumbre en los escenarios actuales se presenta como factor principal que obliga a enfrentar amenazas de carácter sutil, multipolar e indefinido, en donde la inteligencia y la innovación resultarán elementos fundamentales para determinar las soluciones encaminadas a combatirla o anularla.[45]

Conclusiones Parciales

Actualmente el Comando Conjunto de las Fuerzas Armadas se encuentra frente a un entorno complejo, incierto y dinámico y es justamente en esa incertidumbre cuando funciona la prospectiva, que es la herramienta utilizada para el diseño del escenario de las Fuerzas Armadas ecuatorianas. Si bien el futuro es imposible de predecir, la prospectiva es una disciplina científica que nos ayuda a reducir la incertidumbre y desentrañar el futuro, si bien es una disciplina relativamente nueva en nuestro medio, en el mundo se viene aplicando desde inicios del siglo XX.[46]

Una capacidad militar, no es únicamente un arma o un sistema de armas, sino que es algo más, es un conjunto de factores, unos más críticos

[45] Sistema de Planeamiento por capacidades del MIDENA 2016
[46] Plan de Gestión Institucional de FF.AA 2010-2021

que otros, pero que en definitiva son igualmente importantes para la consecución del efecto deseado.

El Planeamiento por Capacidades es un proceso que se establece para un periodo de cuatro años coincidente con el ciclo de gobierno, debiendo ser revisado anualmente. Se trata de un proceso continuo que tiene la flexibilidad suficiente para reaccionar ante nuevos requerimientos y retos de las Fuerzas Armadas.

El Planeamiento por Capacidades se basa en los lineamientos establecidos en el marco legal, en el nivel político a través del Consejo de Seguridad Pública y del Estado quien emite el Plan Nacional de Seguridad Integral.

Cuarto Objetivo Específico y/o Tarea Científica

Determinar las amenazas y riesgos existentes para el Comando de Ciberdefensa.

Introducción

El mundo vive una época de incertidumbre marcada fundamentalmente por eventos violentos, que amenazan a la defensa y seguridad de los Estados de manera permanente. El mismo organismo considera seis grupos de amenazas: las amenazas económicas y sociales (la pobreza, enfermedades infecciosas y la degradación ambiental); los conflictos entre Estados; los conflictos internos (la guerra civil, el genocidio y otras

atrocidades en gran escala); las armas nucleares, radiológicas, químicas y biológicas; el terrorismo; y, la delincuencia organizada transnacional. (Defensa, 2018)

Las amenazas dentro de y procedentes del ciberespacio, como vemos, las redes informáticas son susceptibles de recibir multitud de ataques distintos; éstos formarían parte de las amenazas que el ciberespacio puede tener que soportar como ámbito de comunicación y transmisión de información. Además de estas amenazas, el control, que los sistemas cibernéticos ejercen sobre determinados procesos industriales y financieros proporciona un potencial inmenso de agresión desde el ciberespacio aunque el objetivo este situado fuera de él. En este sentido cabe enfatizar el riesgo a que están sometidos los servicios e infraestructuras críticas, principalmente las instalaciones energéticas de los países desarrollados. Estos sistemas, incluso cuando están convenientemente protegidos y aislados, son un blanco especialmente apetitoso para los intrusos y su potencial, como demostró el virus *stuxnet,* son equivalente al de un ataque convencional masivo.

La posibilidad de hacer daño del ciberespacio no se limita a las acciones ofensivas. La utilización de sus potencialidades por parte de organizaciones terroristas o simplemente, criminales les proporciona un instrumento multiplicador de sus propias capacidades que los convierte en particularmente peligrosos y les da un alcance muy superior al que podrían haber soñado de no contar con estos instrumentos. La notoriedad que buscan estas organizaciones está garantizada por la repercusión mediática que tienen

los incidentes informáticos, especialmente cuando se combinan con acontecimientos de gran relevancia cuya seguridad física haría muy difícil actuar contra ellos directamente.[47]

Conocimiento del Hecho

América Latina, es considerada una zona de paz por la ausencia de conflictos armados interestatales, debido a la adopción de la diplomacia como vía para su solución; sin embargo, no se descarta el empleo del poder militar debido a la confrontación de intereses y al desbalance de las capacidades estratégicas militares en la región.

Por consiguiente, debido a la dinámica permanente de los escenarios geopolíticos, las amenazas varían constantemente con el aparecimiento de nuevos actores y desafíos asociados a factores políticos, sociales, económicos, ambientales y estructurales del Estado, por lo que es necesario mantener un monitoreo permanente de estos elementos, para diseñar medidas preventivas que reduzcan sus potenciales efectos.

El disponer de una capacidad adecuada para vigilar las redes y así detectar de manera oportuna los ataques de red, reduce considerablemente el tiempo de respuesta y la capacidad para recuperar los servicios afectados. Por lo tanto, es fundamental disponer de la correspondiente plataforma de supervisión de la seguridad, entendida ésta como una plataforma especializada que se centra en la gestión de la seguridad de los sistemas de

[47] Estrategias de Ciberseguridad Nacional 2013 España

información y de las redes bajo la responsabilidad de una determinada organización. Un aspecto relevante de estas plataformas es la amplia gama de servicios que pueden ofrecer, como la detección de intrusiones, control y monitorizado de los servicios, gestión inteligente de registros, etc. En ellas se registran y evalúan los fallos del sistema (en relación con la disponibilidad de la infraestructura), así como los incidentes de seguridad (en relación con la integridad y confidencialidad de la información).[48]

El Estado al haber definido sus intereses vitales y estratégicos en la agenda política de la defensa, requiere garantizar la vigencia de los mismos; por tanto, al existir amenazas y riesgos que inciden en la consecución de estos, debe estar en condiciones de protegerlos. Es entonces cuando la defensa se constituye en el instrumento para el empleo de la fuerza ante la amenaza externa que atenta contra estos intereses. (Defensa, 2018)

Análisis

Las Fuerzas Armadas tienen una alta dependencia de las Tecnologías de la Información y las Comunicaciones (TIC)[49], ya que constituyen un pilar básico para poder llevar a cabo las operaciones militares. Sin embargo, este nuevo dominio donde operan estas tecnologías y que se ha venido a denominar el «Ciberespacio», está lleno de un gran número de amenazas que ponen en peligro el éxito de las operaciones militares, así como a las personas que las llevan a cabo. La Ciberseguridad es una necesidad de

[48] Agenda Política de la Defensa 2014-2017
[49] TIC´S: Tecnologías de la Información y las Comunicaciones

nuestra sociedad y de nuestro modelo económico. Dada la influencia de los Sistemas de Información y Telecomunicaciones en la economía y en los servicios públicos, la estabilidad y prosperidad de Ecuador depende en buena medida de la seguridad y confiabilidad del ciberespacio, cualidades que pueden verse comprometida por causas técnicas, fenómenos naturales o agresiones deliberadas.

Tradicionalmente, la seguridad en las TIC en el ámbito militar se ha centrado en la protección de las comunicaciones, aunque hoy en día el uso masivo de sistemas de información hace necesario disponer de una perspectiva más amplia y abordar el problema de una forma integral. De este modo surge el concepto de Seguridad de Gestión de la Información, (SGSI)[50] que se basa en medidas de protección estáticas para los sistemas. (Cornaglia, 2017)

Esta aproximación dinámica, se engloba hoy en el término denominado “Ciberdefensa”, que se puede definir como un conjunto de recursos, actividades, tácticas, técnicas y procedimientos para preservar la seguridad de los sistemas y la información que manejan, así como permitir la explotación y respuesta sobre los sistemas adversarios, para garantizar el libre acceso al ciberespacio y permitir el desarrollo eficaz de las operaciones militares y el uso eficiente de los recursos. (Zea, 2013)

[50] SGSI: Sistema de Gestión de la Seguridad de la Información

Conclusiones Parciales

Las amenazas globales tienen una connotación transnacional que podría afectar a la defensa y seguridad de los Estados. Entre otras, podemos señalar: el terrorismo, narcotráfico y sus delitos conexos, crimen organizado, ciberataques, exploración y explotación ilegal de los recursos marítimos, delincuencia organizada transnacional.

El Estado ecuatoriano concibe intereses nacionales vitales y estratégicos para garantizar la soberanía, propender al desarrollo nacional y alcanzar el bienestar de sus habitantes; por consiguiente, tiene la responsabilidad de proteger su territorio, población y recursos frente a cualquier amenaza que atente contra sus intereses.

Para efectos de la Política de Defensa Nacional y en concordancia con lo señalado en la Declaración sobre Seguridad en las Américas, se conceptualiza a la amenaza como fenómenos, elementos o condiciones de naturaleza antrópica, caracterizada por su capacidad, motivación e intencionalidad de atentar contra los intereses vitales o estratégicos del Estado. (Defensa M. d., 2018)

Los riesgos son considerados como condición interna o externa generada por situaciones de origen natural o antrópico que pudieran afectar a la seguridad y defensa del Estado; su posibilidad de ocurrencia es incierta. En caso de no ser identificados oportunamente o no implementar acciones preventivas podrían traducirse en manifestaciones de peligro. Los riesgos

causados por el hombre pueden convertirse en amenazas una vez que se identifique su motivación, capacidad e intención.

Los flujos migratorios irregulares, causados por la inseguridad social y económica en el lugar de origen de la población afectada, como consecuencia del accionar de factores naturales o antrópicos, obliga al Estado a orientar recursos no planificados para la atención a dichos grupos, con el riesgo de una eventual confrontación social, brote de epidemias, surgimiento de actividades ilegales y otros inconvenientes propios de este fenómeno.

Los ciberataques y vulneración de la infraestructura crítica del Estado, que se basan en la explotación de las debilidades de las redes informáticas, ejecutadas a través de mecanismos tecnológicos de Ciberterrorismo, Ciberdelito, Cibercrimen, Ciberespionaje, e infiltración de los sistemas informáticos, convirtiéndose en un potente instrumento de agresión contra la infraestructura del Estado, lo cual podría comprometer la seguridad nacional.

Capítulo V

Propuesta.

Título de la propuesta

"El Manejo de la Ciberseguridad en las Fuerzas Armadas".

Objetivo de la propuesta.

Desarrollar una guía doctrinaria para el Comando de Ciberdefensa, para que de manera integrada y coordinada permita definir aquellos aspectos que deben ser considerados en base a las capacidades actuales del COCIBER, para de una u otra forma contribuir en el mejoramiento de la capacidad operativa del Comando de Ciberdefensa del CC.FF.AA, ante las nuevas amenazas y riesgos del ciberespacio, así como las Políticas y Estratégicas para neutralizar la amenaza del Ciberterrorismo contra la seguridad del Estado.

Por esta razón el Comando de Ciberdefensa del Comando Conjunto, busca cumplir su misión dentro de tres líneas de operaciones primarias: asegurar, operar y defender el Sistema de Información del Comando Conjunto (SICC)[51], defender a las instalaciones estratégicas críticas de la nación de ataques cibernéticos y proporcionar apoyo cibernético a los Comandos Operacionales que lo requieran. Para ello dispone de personal y unidades entrenadas y equipadas para realizar operaciones en el ciberespacio (OC)[52].

[51] Sistema de Información del Comando Conjunto (SICC)
[52] Operaciones en el Ciberespacio (OC)

Relaciones de comando claramente establecidas son cruciales para asegurar un empleo oportuno y efectivo de las fuerzas, y las OC requieren de unidad de comando y unidad de esfuerzo. Sin embargo, la naturaleza compleja de las OC, donde las fuerzas del ciberespacio pueden estar proporcionando simultáneamente acciones en el nivel nacional y en el nivel de teatro, por lo que se requiere una adaptación de las estructuras tradicionales de C2. Las fuerzas conjuntas, emplean principalmente la planificación centralizada con una ejecución descentralizada de las operaciones.

Las Operaciones de Ciberespacio (OC), requieren una coordinación constante y detallada entre las operaciones nacionales y de teatro, creando una estructura dinámica de C2 que se pueda adatar a los cambios constantes, amenazas emergentes y desconocidas. Ciertas funciones de las Operaciones de Ciberespacio, incluyendo la protección de las redes de Network del Sistema de Información del Comando Conjunto (SICC), así como la búsqueda de las múltiples amenazas, orientan a la planificación y ejecución centralizada para alcanzar los requerimientos múltiples e instantáneos de respuesta. Las OC deben estar integradas y sincronizadas por el comandante apoyado dentro de su concepto operacional, planes y órdenes detallados y en las operaciones conjuntas específicas.

Alcance de la propuesta.

La realización de la presente propuesta, permitirá determinar un mecanismo articulador entre la doctrina y las capacidades que podrían minimizar las posibles amenazas y riesgos existentes en el manejo de la Ciberseguridad en

las Fuerzas Armadas, a fin de establecer los lineamientos doctrinarios ante la necesidad de la protección de la información estratégica del Estado en materia de Defensa y Seguridad.

Además, esto se desarrollará en el marco del contexto nacional, analizando las capacidades en el Ciberespacio que posee el comando de Ciberdefensa en cuanto a las amenazas y riesgos existentes en el País, así como las acciones que debe tomar las Fuerzas Armadas ecuatorianas para la defensa de la Seguridad Nacional.

En el 2018, fue revisada la Política de la Defensa; para posteriormente pasar a ser actualizada, la misma que en la actualidad se sustenta en una concepción estratégica conjunta, organización y estructura operativa flexible, niveles recomendables de alistamiento, con personal militar así como personal civil profesionalmente capacitados e infraestructura física y tecnológica moderna que le permita potencializar las capacidades de Fuerzas Armadas y en especial a las del COCIBER, además, a partir de sus capacidades desarrolladas, apoyar de manera complementaria la consecución de los objetivos de la seguridad integral.

Se debe considerar que el estado a través de sus organismos e instituciones son quienes deben desarrollar las capacidades para ser frente a cualquier amenaza o riego que atente contra la seguridad y estabilidad de este, de igual forma deberá delinear las competencias específicas para cada una para lograr un concepto integrador que permita desarrollar las capacidades de acuerdo a su rol y función. En otro orden, el desarrollo por capacidad permite la

adecuada toma de decisiones en base a lo que puede o no hacer una fuerza o institución, lo que está directamente relacionado con la capacidad, cantidad de medios, recursos y el Estado, este frente a un escenario propuesto que determinará la capacidad que debe disponer para poder cumplir con las misiones constitucionales impuestas en el marco de la legitimidad y legalidad. (Ministerio de Defensa Nacional, 2018)

En la actualidad las amenazas cibernéticas tienen una connotación diferente a la de otras amenazas a la seguridad del Estado; dado que éstas pueden tener diferentes objetivos, pueden ser realizadas por diferentes tipos de actores como el crimen organizado, terroristas u otros Estados, su costo es mínimo y su trazabilidad es complicada. Dada la importancia estratégica de la seguridad en el ciberespacio, la existencia de Ciberamenazas, económicas, asimétricas, anónimas, sin fronteras es imprescindible y prioritario el empleo adicional del personal especializado de FF.AA, en las denominadas guerras cibernéticas, preparadas para: comandar, explotar y mantener un sistema de Ciberdefensa; alcanzar la capacidad de resiliencia, remediación y respuesta ante ciberataques, incidentes o emergencias informáticas, asumir la misión de defender prioritariamente las instalaciones, redes, servicios y equipos físicos y de tecnología de la información cuya interrupción o destrucción tendría un impacto en el eficaz funcionamiento de las instituciones del sector de la Defensa y del Estado.

Es así que la responsabilidad compartida recae no solamente en los entes Estatales, Fuerzas Armadas y Policía Nacional, sino también en los organismos privados que conforman el Estado Ecuatoriano.

Dado el entorno transnacional del Ciberterrorismo y del Cibercrimen es imprescindible también el compromiso de cooperación internacional con base en medidas de confianza mutua y seguridad a fin de contribuir a la paz nacional, regional, continental y mundial. Las nuevas amenazas a la Seguridad del Estado en la quinta dimensión territorial son de naturaleza diversa y tienen un alcance multidimensional. El nuevo dominio territorial, que se ha y está convirtiendo en la nueva dimensión de desarrollo, armonía y confrontación humana exige que los conceptos y enfoques tradicionales de defensa, se deben ampliar, ajustar y crear nuevos conceptos operacionales y de doctrina. No se está descartando de ninguna manera la valiosa experiencia adquirida a través de los años, se está afirmando que es necesario consolidar algunos nuevos enfoques que no necesariamente riñen con las tradiciones de las fuerzas armadas para emplearse de forma adecuada en el ciberespacio.

Los Ciberconflictos han dejado de ser una posibilidad para convertirse en una realidad, de hecho ya han ocurrido acciones de confrontación bélica en el ciberespacio, a lo largo y ancho del planeta. Es tal que, frente a las amenazas y factores de riesgo en el ciberespacio, surge una nueva disciplina, con diversas capacidades de defensa activa, inteligencia y respuesta, la Ciberdefensa.

Los nuevos retos que plantean el ciberespacio y en particular la Ciberdefensa, Fuerzas Armadas sabrán afrontar de forma decidida, en armonía con el apoyo de toda la ciudadanía. Para ello se necesita la legislación adecuada por parte de la Asamblea Nacional que permita desarrollar de mejor forma sus tareas, fortaleciendo la institucionalidad de la ciberfuerza nacional y de la dotación permanente material y equipo necesario. Cabe indicar que las legislaciones y la institucionalización de las ciberfuerzas nacionales son escasas a nivel mundial debido a lo nuevo del tema, pero los riesgos y amenazas son reales, están presentes y no dan tregua.

Desarrollo de la propuesta.

a) Analizar el escenario prospectivo de Fuerzas Armadas en el campo de la Ciberdefensa.

Introducción

Actualmente el Comando Conjunto de las Fuerzas Armadas se encuentra frente a un entorno complejo, incierto y dinámico y es justamente en esa incertidumbre cuando funciona la prospectiva, que es la herramienta utilizada para el diseño del escenario de las Fuerzas Armadas ecuatorianas. Si bien el futuro es imposible de predecir, la prospectiva es una disciplina científica que nos ayuda a reducir la incertidumbre y desentrañar el futuro, si bien es una disciplina relativamente nueva en nuestro medio, en el mundo se viene aplicando desde inicios del siglo XX.[53]

[53] Plan de Gestión Institucional de FF. AA 2010 - 2021

La prospectiva ha sido empleada por gobiernos de varios países, no obstante, es en el campo empresarial donde ha tenido un impacto significativo. En la actualidad, las grandes empresas internacionales, bancos, compañías de negocios y los grandes ejércitos, emplean la prospectiva para el planeamiento de mediano y largo plazo de sus operaciones.

En la actualidad, ya no es posible realizar solo el planeamiento estratégico tradicional, ni en lo político, ni en lo empresarial, ni en lo militar, basados en una “visión” única y siempre deseable para las instituciones; sino que es preciso contar con estrategias claras, además de planes de contingencia basados en diferentes escenarios alternativos, posibles y probables, es aquí donde la prospectiva produce su mayor beneficio.

Conocimiento del Hecho

Las capacidades militares de las Fuerzas Armadas que se sustentan en un conjunto de elementos que producen los efectos operacionales necesarios para cumplir las misiones asignadas y para enfrentarse a los retos futuros no se pueden improvisar. Es importante considerar que el diseño de fuerzas, el fortalecimiento de los sistemas de armas, la investigación tecnológica, el reclutamiento y formación de personal, y el alistamiento operacional, requieren tiempo

de preparación, todo ello bajo las exigencias de un entorno que se encuentra en continuo cambio[54].

A los líderes militares nos corresponde tener una actitud proactiva hacia el cambio y generar los escenarios futuros más deseables y las estrategias para alcanzarlos. La prospectiva es la herramienta que nos ayudará en este esfuerzo a mediano y largo plazo, con un enfoque sistémico, científico, con creatividad e iniciativa.

En ese contexto a las instituciones de seguridad y defensa del Estado ecuatoriano les correspondió redefinir sus capacidades estratégicas para enfrentar las exigencias que plantean el nuevo escenario estratégico, la Constitución del Estado, el Plan Nacional de Desarrollo, la ley de Seguridad Pública y del Estado y las reformas del Estado; lo cual significó revisar y actualizar la estructura, la doctrina, las concepciones de seguridad y defensa, el entrenamiento, el equipamiento, los modelos de gestión operacional, institucional y administrativo.

El crecimiento económico de nuestro país le ha permitido al Estado ecuatoriano disponer de los recursos necesarios para asignarlos al sector de la defensa, por lo que el país cuenta actualmente con unas Fuerzas Armadas disuasivas, mayor equilibrio en el balance militar frente a los países de la región e inmersas en

[54] Plan de Gestión Institucional de FF. AA 2010 - 2021

planes de modernización de sus fuerzas. De forma general, los países miembros de la Organización de Estados Americanos han dado fiel cumplimiento a las “Medidas de Fomento de la Confianza y Seguridad Mutua”, a los “Lineamientos para la elaboración de políticas y doctrina de defensa” y han transparentado plenamente sus metas y objetivos militares, planteados en sus documentos estratégicos, con el objetivo de disponer de unas Fuerzas Armadas disuasivas que permitan mantener un equilibrio militar en la región.[55]

La emisión de una adecuada política pública por parte del Estado, orientó la asignación oportuna de los recursos económicos para la economía de defensa, lo que incidió directamente en la capacidad estratégica de Fuerzas Armadas, lo cual contribuyó al apoyo al desarrollo, a la cooperación con los organismos de seguridad del Estado y gestión de riesgos y a la cooperación internacional (misiones de paz y humanitarias); aumentando significativamente el liderazgo en todos los niveles, lo que indirectamente tuvo un efecto positivo en la moral del personal de Fuerzas Armadas, reflejado en un adecuado cumplimiento de su misión constitucional.

Análisis

En el ámbito internacional se han producido cambios en la estructura geopolítico-mundial con tendencias a la globalización y la fragmentación de los estados-nación; han aparecido nuevos espacios

[55] Plan de Gestión Institucional de FF. AA 2010 - 2021

geopolíticos y nuevas alianzas estratégicas, la conformación de espacios económicos regionales y extensas regiones marginales.

Los conflictos armados entre los Estados son menos probables; sin embargo, el mundo se ha tornado más impredecible, inestable, ambiguo y complejo; en la actualidad y en el futuro los conflictos internos con repercusiones regionales, son más frecuentes, lo que privilegia la atención a la cooperación interestatal, interinstitucional e interagencial, permitiendo a los Estados mejorar su capacidad de lucha contra las nuevas amenazas, especialmente aquellas relacionadas con: los grupos ilegales armados, la inseguridad ciudadana, el tráfico de drogas, la trata de personas, el crimen organizado transnacional, la piratería marítima, la contaminación ambiental, el cambio climático y los desastres naturales.[56]

Asimismo, la constante amenaza ciberespacial, con la posibilidad de colapsar e incluso dañar físicamente los sistemas de información a lo que se suman: el espionaje, sabotaje y el rastreo cibernético, ejecutados no sólo por *hackers, crackers, script bunnies, insiders* informáticos, sino de: terroristas, organizaciones criminales y extremistas políticos, movimientos sociales, religiosos, servicios de inteligencia y fuerzas militares extranjeras.

[56] Plan de Gestión Institucional de FF.AA 2010-2021

Al interior de la institución se ha completado la reestructuración de Fuerzas Armadas, proceso que ha permitido un dimensionamiento de fuerza acorde al nuevo escenario estratégico, implementando una organización dinámica y flexible, que facilita cumplir las misiones de las Fuerzas Armadas mediante la integración sinérgica y coordinación de los organismos de planificación, preparación, empleo y apoyo de manera efectiva; se ha consolidado el sistema de inteligencia militar, el sistema de salud y de seguridad integral, también se ha alcanzado la reubicación y conformación de unidades en fuertes o bases militares, se evidencia una organización con modelos de concentración regional, unidades orgánicamente completas, de cuadros profesionales, interoperables, flexibles con capacidad de despliegue rápido y empleo conjunto en cualquier parte del territorio nacional, debidamente dotadas y tecnológicamente bien equipadas, en todos sus sistemas operativos, y en condiciones de enfrentar los nuevos desafíos tales como: los problemas derivados de la inseguridad, la afectación psicosocial, el deterioro al ambiente y la constante amenaza ciberespacial.[57]

En lo internacional, existe fiel acatamiento a las diferentes resoluciones establecidas por el sistema de supervisión del Departamento de Desarme de la Secretaría General de la Organización de las Naciones Unidas (ONU); asimismo, a las resoluciones de la Organización de Estados Americanos (OEA), de la

[57] Plan de Gestión Institucional de FF.AA 2010-2021

Unión de Naciones de América del Sur (UNASUR) y del Consejo de Defensa Suramericano (CDS), de la Comunidad Andina (CAN) y de otros foros, regímenes y mecanismos internacionales de seguridad y defensa, que tienen relación con la cooperación militar, el gasto militar, adquisición de armas y las medidas de fomento de la confianza y seguridad mutua.

Por otra parte, la consolidación del Consejo Sudamericano de la Defensa, ha generado estabilidad en la región volviendo menos probables los conflictos convencionales, reduciendo así significativamente el nivel de conflictividad en toda la región. Las Fuerzas Armadas de los países miembros de la UNASUR cuentan con políticas claras con relación a la implementación de medidas de confianza y a la transparencia y estandarización de los gastos militares; se hace referencia a pesar de que nuestro país dejo de ser miembro desde el 2019. Las diferentes controversias (marítimas o territoriales) entre Estados son sometidas a las instancias internacionales correspondientes para su tratamiento y su análisis, el mismo que se enmarca en las normas jurídicas apegadas al derecho internacional.

La aplicación de la Ciberdefensa en la seguridad nacional, se ha visto necesario que dentro del ciberespacio se desarrollan dos tipos de operaciones: las de Ciberseguridad orientadas a minimizar el nivel de riesgo al que están expuestos los ciudadanos ante amenazas de

índole cibernético y las de Ciberdefensa encaminadas a garantizar el sentido de seguridad del Estado Nacional.

Es evidente que en el siglo anterior los avances en las técnicas de la información y de las comunicaciones, se reflejan en ingenios usados en el cuarto dominio denominado espacial y con mayor impacto en el quinto dominio el ciberespacio, el mismo que además de pulverizar las barreras de tiempo y distancia obligo a establecer nuevos esquemas de defensa a las Fuerzas y Cuerpos de Seguridad para enfrentar los nuevos desafíos del siglo XXI en un teatro de operaciones virtual.

La Constitución de la República del Ecuador, posiciona al ser humano y su bienestar como objetivo central de todas las acciones institucionales entre las cuales consta el garantizar la seguridad integral y la defensa del Estado. Determina que las Fuerzas Armadas son una institución de protección de los derechos, libertades y garantías de los ciudadanos y tiene como misión fundamental la defensa de la soberanía e integridad territorial. Las Fuerzas Armadas ejercen el control y la protección del territorio ecuatoriano que comprende el espacio continental y marítimo, las islas adyacentes, el mar territorial, el archipiélago de Galápagos, el suelo, la plataforma submarina, el subsuelo y el espacio supra yacente continental, insular y marítimo (Defensa P. d., 2018).

La defensa nacional en el Ecuador, es un bien público y como tal requiere del accionar de todas las instituciones del Estado para su preservación; por tanto, incluye actividades políticas, psicosociales, económicas y militares para enfrentar situaciones que comprometen los intereses nacionales.

La actitud estratégica del Estado ecuatoriano es defensiva, fundamentada en la prevención y la alerta temprana. Considera el empleo de la fuerza militar en caso de una inminente amenaza externa que ponga en riesgo la integridad de los ciudadanos, del territorio y de los intereses estratégicos y vitales del Estado. Cuenta con unas Fuerzas Armadas que poseen capacidades estratégicas conjuntas para acciones de preparación, prevención, disuasión defensiva, defensa y cooperación internacional para el empleo militar ante amenazas y riesgos, sustentadas en el concepto de legítima defensa.

El Ecuador es un Estado que se desenvuelve en el contexto internacional bajo principios de soberanía y cooperación; fomenta la convivencia pacífica y la solución de conflictos por la vía diplomática, por lo que reconoce el derecho internacional y las medidas de confianza mutua; contribuye al mantenimiento de la paz entre los Estados sin desestimar el uso del poder nacional cuando los intereses nacionales se vean afectados o en peligro[58].

[58] Política de la Defensa 2018

Las Fuerzas Armadas en el marco del cumplimiento de su misión constitucional y tareas complementarias se sujetan a la norma jurídica vigente, respeto a los derechos humanos, al Derecho Internacional Humanitario, equidad de género y la protección del ambiente. Las Fuerzas Armadas participan en el desarrollo económico del Ecuador como generadoras de encadenamiento productivo, a través de las actividades vinculadas a la industria de la defensa y a los institutos de investigación de las Fuerzas Armadas, cuyas capacidades coadyuvan al desarrollo nacional y a la disminución de la dependencia externa en el ámbito tecnológico y científico.

La defensa nacional, constituye un componente esencial de la seguridad nacional que, articulada con la seguridad pública, la política exterior, el apoyo del sistema de inteligencia nacional, garantiza la defensa de la soberanía e integridad territorial y la protección de la población y de los recursos; con los mecanismos de cooperación internacional contribuye a crear un entorno nacional y regional estable y seguro.

El Estado al haber definido sus intereses vitales y estratégicos requiere garantizar la vigencia de los mismos; por tanto, al existir amenazas y riesgos que inciden en la consecución de estos, debe estar en condiciones de protegerlos. Es entonces cuando la defensa

se constituye en el instrumento para el empleo de la fuerza ante la amenaza externa que atenta contra estos intereses.

La defensa se ejerce con todos los recursos del país, pero las Fuerzas Armadas con sus capacidades, estructura y doctrina; son el medio principal para mantener la soberanía e integridad territorial, proteger a la población y los recursos ante amenazas y riesgos cada vez más complejos y difusos.

La defensa nacional tiene una relación directa con la política exterior del Estado, a fin de garantizar la coherencia de las acciones que se desarrollen en los ámbitos militar y diplomático para el cumplimiento de sus objetivos. Se orienta por las decisiones soberanas de la política exterior, fundamentadas en los principios del derecho internacional, en la realidad política, económica y social interna y en la situación del entorno internacional. La defensa nacional está orientada a garantizar la paz, la estabilidad y la prosperidad que permitan lograr un desarrollo económico y social sostenible y sustentable, contribuye así a la seguridad integral y al fortalecimiento de la unidad nacional en la diversidad.

Para el cumplimiento de su gestión el sector de la Defensa se alinea predominante al objetivo 1 que dice: “Ejercer el control efectivo del territorio nacional: continental, insular, espacios acuáticos 2 y aéreos; así como de la infraestructura y recursos de las áreas

estratégicas” y al objetivo 3 que dice: “Fortalecer las capacidades estratégicas conjuntas de las Fuerzas Armadas que sean indispensables para mantener una capacidad de disuasión y defensa de la integridad territorial y de la soberanía nacional”, del documento base que provee el lineamiento estratégico de la política pública denominado Plan de Desarrollo Nacional y que se plasman en estrategias para asegurar el ciberespacio:

a. Desarrollar capacidades para la Ciberdefensa.
b. Desarrollar nuevas capacidades estratégicas conjuntas para contribuir a la paz integral.
c. Generar una coordinación efectiva con los organismos competentes para proteger los Recursos Estratégicos del Estado.
d. Proteger la infraestructura, redes estratégicas e información electrónica, en el ámbito de la Defensa.
e. Fortalecer los mecanismos interinstitucionales para hacer frente a las amenazas cibernéticas que atentan contra la seguridad del Estado.

Estas estrategias impulsan a que el sector de la Defensa y Fuerzas Armadas como órgano operativo, coadyuven al Estado ecuatoriano en el desarrollo de la capacidad de Ciberdefensa, a través de un conjunto de medidas y gestiones destinadas a alcanzar las condiciones de seguridad en el ciberespacio. Para hacer frente a

los nuevos requerimientos es necesario incrementar capacidades específicas en función de cuatro componentes fundamentales: Estructura organizacional, Procesos probados, Personal altamente entrenado y Tecnología de vanguardia, orientados a iniciar el desarrollo de una adecuada capacidad estratégica conjunta de Ciberdefensa para mitigar o anular el interés sobre blancos civiles y militares propios de posibles adversarios o potenciales enemigos.

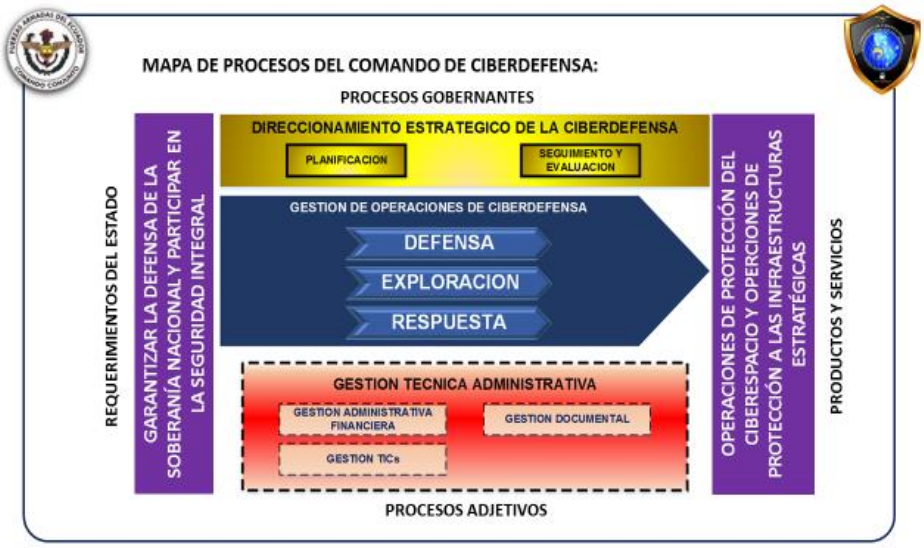
Para el cumplimiento de competencias, deberes y responsabilidades en todo el ámbito nacional, el Ecuador utiliza como guía determinante un marco legal establecido, la Constitución de la República, el Artículo 158 define como misión fundamental de Fuerzas Armadas la defensa de la soberanía y la integridad territorial. Las FF.AA. del Ecuador siempre han estado dispuestas a cumplir con sus deberes y los han cumplido, desde las mismas gestas emancipadoras del siglo XX, a través de la institucionalización del ejército desde la fecha épica de 10 de agosto de 1809, de la Marina Militar establecida el 3 de noviembre de 1832 por el Congreso Constitucional del Ecuador, de la Aviación Militar ecuatoriana que considera su inicio el 27 de octubre de 1920 fecha en la cual el Congreso Nacional emitió el decreto para la formación e las escuelas de aviación en Quito y Guayaquil y ahora sumada a las anteriores la Ciberdefensa creada mediante Acuerdo 281 del 12 de septiembre del 2014 por el Ministerio de Defensa Nacional (M.D.N.).

En cumplimiento al Artículo 7 del Acuerdo 281 del M.D.N.: “El Comando de Ciberdefensa, se conformará como un Comando del CC.FF.AA., integrado por personal técnico y operativo, civil y militar. Tendrá la misión de operar las capacidades de Defensa, Exploración y Respuesta en el espacio cibernético, para proteger y defender la infraestructura crítica e información estratégica del Estado”[59], el Comando Conjunto de FF.AA., conformo un Comando de Ciberdefensa, la organización despliega su razón de ser, evidencia su mapa de procesos que se encuentra estructurada administrativamente por requerimientos fundamentales de la ciudadanía y del Estado para garantizar la defensa de la soberanía nacional y participar en la seguridad integral, requerimientos que son traducibles en procesos sustantivos o misionales de operaciones de defensa y exploración en el ciberespacio en forma permanente, para proteger la infraestructura crítica del Estado, y en operaciones de disuasión y respuesta para degradar o neutralizar a los antagonistas internos y/o externos, ver figura N° 2.

[59] Orden Ministerial No. 188 del 24 de septiembre 2014, Acuerdo Ministerial No. 281

Figura N° 9.

Mapa de procesos del Comando de Ciberdefensa[60]



El escenario de la defensa actual define para FF.AA. cuatro misiones complementarias entre sí:

a. Garantizar la defensa de la soberanía e integridad territorial.
b. Participar en la seguridad integral.
c. Apoyar el desarrollo nacional en el ejercicio de las soberanías.
d. Contribuir a la paz nacional, regional y mundial.

Para garantizar la defensa de la soberanía e integridad territorial como misión fundamental, el concepto de operaciones incluye actualmente operaciones militares de vigilancia y control en los espacios terrestre, marítimo, aéreo y las operaciones de protección

[60] Tomado de Aplicación de la Ciberdefensa en seguridad nacional del COCIBER 2015

del espacio cibernético mediante acciones de prevención, disuasión, protección, exploración y respuesta ante eventuales amenazas, riesgos e incidentes en el ciberespacio.

La participación en la seguridad integral, conlleva la tarea de realizar operaciones de protección a las áreas de infraestructura estratégica a nivel del territorio continental, marítimo, insular, aéreo y cibernético cuya criticidad depende del impacto que puede ocasionar la interrupción o destrucción de las instalaciones asociadas a las infraestructuras críticas tales como redes eléctricas y de telecomunicaciones, servicios que afecten las actividades económicas, productivas, laborables, la gobernabilidad y los derechos y deberes de los ciudadanos.

La gran dinámica del desarrollo nacional, se ha traducido, por una parte, en el fortalecimiento de la automatización e interconexión de redes, de procesos de sistemas de control del tráfico terrestre, marítimo y aéreo, de la generación eléctrica, del sistema de agua potable, del sistema de salud, de las rentas internas, del área financiera, de compras públicas, entre otros. También la dinámica nacional se manifiesta en el fortalecimiento de las FF.AA., en sus sistemas operativos de aplicaciones informáticas para Inteligencia, Operaciones, Personal, Logística, Abastecimientos, Sanidad, Finanzas, Presupuesto, entre otros.

Pero por otra parte esa dinámica nacional y mundial ha creado y dejado expuestas muchas vulnerabilidades en el ciberespacio de la sociedad en su conjunto. La protección y defensa de los recursos e información estratégica de las FF.AA. y del Estado deben responder a un concepto integral de defensa física y virtual, quedando lejos el concepto operacional de emplear exclusivamente equipos cinéticos y guardias bien entrenados para proteger la infraestructura crítica controlada por las TIC's.

Para apoyar al desarrollo nacional en el ejercicio de las soberanías tales como la tecnológica entre otras, FF.AA. disponen de equipamiento perfeccionado por personal militar, inmerso en la investigación y desarrollo de tecnología militar, naval y aeroespacial, incursionando además en proyectos de software, aviones no tripulados, plataformas de gran altura. Concomitante con el impulso de la Ciberdefensa, algunos recursos, deben orientarse a producir ingenios disuasivos a las actividades hostiles en el ciberespacio para proteger nuestros datos, evitar el uso de los datos propios de los adversarios y fortalecer las capacidades específicas de mando y control de nivel estratégico, operativo y táctico en cada Fuerza, sostener en niveles mínimos de riesgos asociados a las redes de comunicaciones, informática y protección de la información, recursos extremadamente útiles para contribuir en la defensa y seguridad integral del Estado.

Ante los intereses del país, de la sociedad y del Comando de Ciberdefensa del Comando Conjunto de FF.AA. en particular, la tarea de formar y capacitar a oficiales, tropa y personal civil en la defensa de la soberanía digital del Estado, la oferta academia universitaria del país debe incluir carreras que permitan cumplir con los siguientes objetivos del Estado:

a. Implementar y sostener la capacidad de Ciberdefensa.
b. Ser actores destacados en la implementación de la capacidad de defensa en el ciberespacio.
c. Ampliar el conocimiento científico y tecnológico en el campo aeroespacial.
d. Enfrentar un ambiente externo de acelerada evolución tecnológica y alta competitividad.
e. Formar e innovar y contribuir en la autonomía tecnológica
f. Articular con instituciones convergentes, con la industria y con otros segmentos de la sociedad esenciales para el desarrollo de las actividades orientadas a la defensa en el ciberespacio.
g. Inserción proactiva en el desarrollo científico y tecnológico orientado a la industria aeroespacial y de la defensa.

Dado el entorno transnacional es imprescindible el compromiso de cooperación internacional, a fin de contribuir a la paz nacional, regional, continental y mundial. Las nuevas amenazas a la Seguridad

del Estado en la quinta dimensión territorial son de naturaleza diversa y tienen un alcance multidimensional. Los Ciberconflictos han dejado de ser una posibilidad para convertirse en una realidad, tal que, frente a las amenazas y factores de riesgo en el ciberespacio, surge una nueva disciplina, con diversas capacidades de defensa activa, inteligencia y respuesta, la Ciberdefensa.

Conclusiones Parciales

Impulsar la gestión integral a nivel nacional, de la Ciberseguridad, con una visión holística y participación de los responsables gubernamentales de establecer las normas, la política, la organización, y la cooperación a nivel nacional e internacional. La responsabilidad compartida recae no solamente en los entes Estatales, Fuerzas Armadas y Policía Nacional sino también en los organismos privados que conforman en estado ecuatoriano. Uno de los mayores riesgos contra la Seguridad Nacional es no considerar la Ciberdefensa como una realidad de la seguridad integral del estado.

Las Fuerzas Armadas constituyen el componente militar de la defensa, en el marco de la seguridad, cuyas misiones complementarias no eximen a la sociedad civil y a las demás organizaciones e instituciones públicas y privadas, de compartir el compromiso para alcanzar la soberanía, la defensa de la integridad territorial y de la paz nacional. El poco desarrollo de la cultura de seguridad nacional, dificulta la concientización de que la defensa no

es de exclusiva responsabilidad militar sino un concepto y sistema integral en el cual se interrelacionan las esferas política, parlamentaria, judicial, administrativa, económica, educativa y financiera.

Los nuevos retos que plantean el ciberespacio y en particular la Ciberdefensa, Fuerzas Armadas sabrán afrontar de forma decidida, en armonía con el apoyo de toda la ciudadanía. Para ello se necesita la legislación adecuada por parte de la Asamblea Nacional que permita desarrollar de mejor forma sus tareas, fortaleciendo la institucionalidad de la ciberfuerza nacional y de la dotación permanente material y equipo necesario. Cabe indicar que las legislaciones y la institucionalización de las ciberfuerzas nacionales son escasas a nivel mundial debido a lo nuevo del tema, pero los riesgos y amenazas son reales, están presentes y no dan tregua.

b) Analizar los aspectos doctrinarios que deben ser tomados en consideración para el desarrollo de las capacidades del ciberespacio.

Introducción

El Ministerio de Defensa Nacional, estableció en la Agenda Política de la Defensa Nacional, la necesidad de la protección de la información estratégica del Estado en materia de Defensa, incluyendo la protección de la infraestructura, las redes estratégicas y la información electrónica; el desarrollo de las capacidades de

Ciberdefensa; y el fortalecimiento de los mecanismos inter institucionales para hacer frente a las amenazas cibernéticas, por lo que mediante Acuerdo Ministerial No 281 de fecha 24 de septiembre del 2014, acordó la creación del Sistema de Ciberdefensa del Ministerio de Defensa Nacional, como un mecanismo articulador de las instancias pertinentes, para la implementación de las políticas y estrategias de Ciberdefensa a nivel nacional. (Nacional, 2018)

Los aspectos contenidos en este documento, pueden constituirse en una guía para el Comando de Ciberdefensa, para que, de manera integrada y coordinada por el Estado Mayor del Comando Conjunto, permitan al CFC[61] y sus comandantes operativos, la integración de los aspectos inherentes a las Operaciones en el Ciberespacio, con la planificación para el cumplimiento de los requerimientos, tareas y misiones contempladas en su plan de operaciones.

La doctrina que se plantea es en base a las operaciones de Ciberdefensa de las Fuerzas Armadas de Estados Unidos, la cual busca definir aquellos aspectos que deben ser tomados en consideración para el desarrollo de las capacidades del ciberespacio y para la planificación y ejecución de las operaciones en el ciberespacio por parte del Comando de Ciberdefensa del Comando Conjunto de las FF.AA., en apoyo a las otras operaciones militares que se planifican y ejecutan por parte de una fuerza conjunta, en una

[61] Comandante de la Fuerza Conjunta: CFC

Zona/ Teatro de Operaciones Conjunto, para la consecución de los objetivos asignados.

Conocimiento del Hecho

El Ministerio de Defensa Nacional velará por el fortalecimiento de las capacidades operativas pertinentes y desarrollará las políticas específicas en el ámbito aeroespacial, Ciberdefensa, gestión de riesgos, seguridad integral, empleo progresivo de la fuerza contra vuelos ilegales y misiones de inteligencia.[62]

La mayoría de las acciones del ciberespacio utilizan el ciberespacio para facilitar otros tipos de actividades, que emplean las capacidades del ciberespacio para completar otras tareas que no son parte de las tres misiones de las Operaciones del Ciberespacio: Operaciones Ofensivas en el Ciberespacio (OOC)[63], Operaciones Defensivas en el Ciberespacio (ODC)[64] y las operaciones del Comando Conjunto (OCC)[65].

Esa utilización incluye acciones como la operación de un sistema de C2[66] o de un sistema logístico, él envió de un email para apoyar un objetivo de información, el uso del internet para completar un curso de entrenamiento online, o para desarrollar un briefing. Otros usuarios,

[62] Agenda Política de la Defensa 2018
[63] OOC: Operaciones Ofensivas en el Ciberespacio
[64] ODC. Operaciones Defensivas en el Ciberespacio
[65] OCC. Operaciones del Comando Conjunto
[66] Comando y Control: C2

que pueden ser usuarios no autorizados de network, personal del Comando Conjunto que no necesita una autorización especial para utilizar las capacidades del ciberespacio, etc. En el ciberespacio la mayoría de las vulnerabilidades del sistema del Comando Conjunto, pueden estar expuestas y ser explotadas por nuestros adversarios. El desafío es entrenar a todos los usuarios del Comando Conjunto para comprender el significado de las amenazas del ciberespacio, y a reconocer las tácticas de la amenaza para que el uso del ciberespacio no genere un riesgo innecesario a las operaciones. La protección del ciberespacio del Comando Conjunto mediante el establecimiento de una cultura de prevención de las vulnerabilidades, particularmente mediante políticas, prácticas y entrenamiento, es crítico para el éxito de todos los tipos de operaciones permitidas en el ciberespacio.

Análisis

Desarrollar una guía doctrinaria para el Comando de Ciberdefensa, para que de manera integrada y coordinada con las demás Fuerzas puedan definir aquellos aspectos que deben ser considerados para el desarrollo de las capacidades actuales del Comando de Ciberdefensa para contribuir en el mejoramiento de la capacidad operativa del Comando de Ciberdefensa del CC.FF.AA, ante las nuevas amenazas y riesgos del ciberespacio, así como las Políticas y Estrategias para neutralizar la amenaza del Ciberterrorismo contra la seguridad del Estado.

La autoridad para la planificación ejecución de Operaciones militares en el ciberespacio está establecida dentro de las políticas emitidas por el Ministerio de Defensa, así como en las órdenes recibidas que autorizan al Comando de Ciberdefensa a la ejecución de estas operaciones.

Los responsables por la planificación y ejecución de las OC[67], deberán conocer y aplicar los principios y normas de empleo descritos en esta propuesta, que son de carácter general, producto de experiencias acumuladas por otras fuerzas armadas, y que, sumados a las experiencias propias, permitirán el desarrollo de las capacidades en el ciberespacio para la planificación y ejecución de las Operaciones en el Ciberespacio.

Operaciones militares en y dentro el Ciberespacio.

Las OC, consisten en el empleo de capacidades en el ciberespacio donde el propósito primario es alcanzar objetivos en o dentro del ciberespacio. Las OC comprenden la inteligencia militar, inteligencia nacional y las actividades ordinarias del Comando Conjunto y del Ministerio de Defensa, dentro y a través del ciberespacio. A pesar de que los comandantes deben ser advertidos sobre el impacto potencial de las operaciones que desarrolla el Comando de Ciberdefensa sobre sus operaciones, el componente

[67] OC: Operaciones en el Ciberespacio

militar de las OC, es el único que debe ser guiado por esta doctrina y es el focus para esta publicación. Las operaciones militares en el ciberespacio están organizadas en misiones ejecutadas mediante una combinación de acciones específicas que contribuyen a la consecución de los objetivos del comandante.

a. Misiones en el Ciberespacio.

Existen tres tipos de misiones que cubren completamente las actividades de las fuerzas del ciberespacio. La ejecución exitosa de las OC requiere de la integración y sincronización de todas estas misiones. Las misiones militares del ciberespacio y sus acciones relacionadas, serán normalmente autorizadas a través de una orden militar (orden ejecutoria, orden de operaciones, orden verbal, etc). Las misiones de las OC[68] son categorizadas en OOC[69], ODC[70] y OCC[71], basados solamente en la intención u objetivo buscado por la autoridad que lo requiere, y no por las acciones del ciberespacio ejecutadas, el tipo de autoridad militar utilizada, las fuerzas asignadas a la misión, o las capacidades del ciberespacio utilizadas. Algunas órdenes pueden cubrir múltiples tipos de misiones.

[68] Operaciones en el Ciberespacio: OC
[69] Operaciones Ofensivas en el Ciberespacio: OOC
[70] Operaciones Defensivas en el Ciberespacio: ODC
[71] Operaciones del Comando Conjunto: OCC

(1) Operaciones del Comando Conjunto.

Las misiones de operaciones del Comando Conjunto incluyen acciones operacionales que se toman para asegurar, configurar, operar, extender, mantener y sostener el Ciberespacio del Comando Conjunto y para crear y preservar la confidencialidad, disponibilidad, e integridad del ciberespacio de la red de información del Comando Conjunto. Esto incluye acciones proactivas para la seguridad del ciberespacio, para prevenir las vulnerabilidades del sistema. Incluye, además, el establecimiento de redes tácticas, desplegando fuerzas para extender las redes existentes, acciones de mantenimiento y otras acciones necesarias para el sostenimiento del sistema, la detección de la operación de equipos rojos y otras formas de evaluación de la seguridad. Las operaciones del sistema de información del comando conjunto, están centradas en la red y son agnósticas: las fuerzas del ciberespacio y la fuerza de trabajo que emprenden esta misión, deben esforzarse por evitar que todas las amenazas tengan un impacto negativo en una red o sistema en particular, ellas están asignadas para proteger el sistema. Ellas están informadas sobre la amenaza y utilizan toda la inteligencia disponible sobre amenazas específicas, para incrementar el nivel de seguridad de la red.

(2) Operaciones defensivas en el Ciberespacio (ODC).

Las misiones de ODC, son ejecutadas para defender el sistema de información del Comando Conjunto (SICC)[72], u otros ciberespacios que hayan sido ordenados defenderlos, de las actividades de la amenaza en el ciberespacio. Específicamente, son misiones destinadas a preservar la habilidad para la utilización del ciberespacio azul, y proteger las bases de datos, redes, equipos que utilizan el ciberespacio para su operación, y otros sistemas designados, evitando o impidiendo el desarrollo de actividades maliciosas en el ciberespacio. Esto caracteriza a las ODC, que vencen las amenazas específicas que hayan sobrepasado, violado o intenten violar las medidas de seguridad de las operaciones del SICC. Las ODC son específicas en contra de las amenazas y frecuentemente apoyan la consecución exitosa de los objetivos de la misión. Las ODC son conducidas en respuesta a amenazas específicas de ataque, explotación, y otros efectos de las actividades maliciosas del ciberespacio y permitir que la información requerida para la maniobra, búsqueda de inteligencia, operaciones de CI, y otras pueda fluir con seguridad. Las ODC incluyen maniobrar e

[72] Sistema de Información del Comando Conjunto: SICC

interceptar las acciones que el adversario está tomando o pensando en ejecutar en contra de los elementos defendidos en el ciberespacio, o para responder ante una amenaza interna o externa inminente en el ciberespacio.

(a).- Operaciones defensivas en el Ciberespacio – Medidas defensivas internas (ODC-MDI).

Las ODC-MDI, son formas de misiones de ODC autorizadas que se toman o ejecutan para defender la red o una porción del ciberespacio. Las ODC-MDI del SICC, son autorizadas por una orden formal e incluye acciones defensivas del ciberespacio para reconfirmar dinámicamente o restablecer la seguridad del ciberespacio del Comando Conjunto que ha sido degradado, comprometido o amenazado y permitir el acceso que permita el cumplimiento de las misiones militares.

(b).- Operaciones defensivas en el Ciberespacio- Acciones de respuesta (ODC-AR).

Las ODC-AR son formas de misiones de ODC en donde las acciones externas tomadas para la defensa de la red o de una porción del ciberespacio, son tomadas sin la autorización o el permiso del propietario del sistema afectado. Las ODC-AR, se

ejecutan normalmente en el ciberespacio extranjero, y pueden incluir misiones que incrementen el nivel del uso de la fuerza, daño físico o destrucción de los sistemas enemigos y dependiendo del contexto operacional, como la apertura inminente de hostilidades, el grado de certeza sobre la amenaza, el daño que esta ha causado o se espera que cause, así como las consideraciones sobre la política nacional.

(3) Ofensivas en el Ciberespacio (OOC).

Las OOC, son misiones diseñadas para proyectar el poder en y a través del ciberespacio extranjero, mediante las acciones tomadas en apoyo de los comandantes operacionales o de los intereses nacionales. Las OOC pueden afectar exclusivamente las funciones en el ciberespacio de los blancos adversarios o crear efectos de primer orden en el ciberespacio para iniciar una cascada controlada de efectos en los dominios físicos, para afectar a los sistemas de armas, proceso de C2, nudos logísticos, blancos de alto valor (BAV), etc. Todas las OOC conducidas por fuera del ciberespacio azul, con la intención del comandante diferente a la defensa del ciberespacio azul, frente a una amenaza inminente, son misiones OOC. Al igual que las misiones ODC-AR, algunas OOC pueden incluir

acciones que elevan el nivel del uso de la fuerza, con daño físico o destrucción de los sistemas enemigos. Los efectos específicos creados dependen del amplio contexto operacional, como la existencia o inminencia de hostilidades abiertas o consideraciones políticas nacionales. Las misiones OOC requieren de una orden militar coordinada y cuidadosas consideraciones sobre el alcance, reglas de enfrentamiento y objetivos medibles o cuantificables.

b. Acciones en el Ciberespacio.

La ejecución de cualquier OOC, ODC u operaciones de protección del SICC, requieren de la ejecución de acciones específicas en el nivel táctico o tareas que empleen las capacidades del ciberespacio para crear efectos en el ciberespacio. Todos los objetivos de las misiones en el ciberespacio son alcanzados mediante la combinación de una o más de dichas acciones, que son definidas exclusivamente por el tipo de efectos que va a crear. La planificación, autorización y evaluación de dichas acciones, requiere que el comandante y su staff entiendan claramente que acciones han sido autorizadas dentro de la misión recibida.

(1) Seguridad en el ciberespacio.

Las acciones de seguridad en el ciberespacio, son acciones tomadas dentro del ciberespacio protegido, para prevenir un acceso no autorizado, las explotación o el daño de computadores, sistemas de comunicación electrónicos y otros medios de TI, incluyendo plataformas de información tecnológicas PIT, así como toda la información en ellas contenidas, para asegurar su disponibilidad, integridad, autenticación, confidencialidad y el no repudio.

(2) Defensa en el Ciberespacio.

Las acciones de defensa en el ciberespacio, son tomadas dentro del ciberespacio protegido, para vencer amenazas específicas que hayan violado o intenten violar las medidas de seguridad del ciberespacio e incluyen acciones para detectar, caracterizar, contrarrestar y mitigar las amenazas, incluyendo malware o actividades no autorizadas de los usuarios, y para restaurar el sistema a una configuración segura.

(3) Explotación del ciberespacio.

Las acciones de explotación del ciberespacio incluyen actividades de inteligencia militar, maniobra, colección de información, y otras actividades relacionadas requeridas

para planificar operaciones militares futuras. Las acciones de explotación del ciberespacio son tomadas de como parte de las misiones de OOC o ODC-AR e incluyen todas las acciones que se ejecutan en los ciberespacios gris y rojos que no crean efectos de ataque en el ciberespacio. Incluyen actividades para obtener inteligencia y apoyar la preparación operacional del ambiente para las operaciones decurrentes y futuras, mediante acciones como las destinadas a ganar y mantener acceso a las redes, sistemas y nodos de valor militar; maniobrar para obtener una posición ventajosa; y, posicionar las capacidades del ciberespacio para facilitar las acciones subsiguientes. La explotación del Ciberespacio apoya además las operaciones decurrentes y las futuras, mediante la colección de información, incluyendo el mapeo del ciberespacio rojo y gris, para apoyar la alerta situacional; descubrir vulnerabilidades, permitir el desarrollo de blancos, y apoyar la planificación, ejecución y evaluación de las operaciones militares.

(4) Ataque en el ciberespacio.

Las acciones de ataque en el ciberespacio crean efectos de negación notables (Ej., degradación, interrupción, o destrucción) en el ciberespacio o manipulan para orientar dichos efectos en los dominios físicos. A pesar de que las

acciones de explotación en el ciberespacio, que a menudo están destinadas a permanecer en la clandestinidad para ser efectivas, las acciones de ataque en el ciberespacio pueden ser aparentes para los operadores de los sistemas o usuarios, ya sea inmediatamente o eventualmente, ya que ellas remueven ciertas funcionalidades de los usuarios. Las acciones de ataque en el ciberespacio son una forma de fuegos, son tomadas como parte de las misiones de OOC o de las ODC-AR, y deben ser coordinadas con los otros departamentos y agencias, así como cuidadosamente sincronizadas con los fuegos planeados en los dominios físicos. Incluyen acciones para:

(a) Negar. Prevenir el acceso a, la operación de, o la disponibilidad de función de un blanco por un nivel específico, para un tiempo específico, mediante:

1. Degradar. Negar el acceso a, o la operación de un blanco a un nivel representado como un porcentaje de su capacidad. El nivel de degradación es especificado. Si un tiempo específico es requerido, este también debe ser especificado.

2. Interrumpir. Negar completamente el acceso a, de manera temporal, o la operación de un blanco por un periodo de tiempo. El tiempo de inicio y

finalización de la interrupción estará normalmente especificado. Las interrupciones pueden ser consideradas un caso especial de degradación cuando el nivel de degradación alcanza el 100%.

3. Destruir. Negar el acceso de manera completa e irreparable a, o la operación de un blanco. La destrucción maximiza el tiempo y la cantidad de negación. Sin embargo, la magnitud de la destrucción estará acorde con la expansión del conflicto, ya que muchos blancos, dados el tiempo necesario y los recursos pueden ser reconstituidos.

(b) Manipular. La manipulación como una forma del ataque en el ciberespacio, controla o cambia la información, sistemas de información, y/o las redes en los ciberespacios grises o rojos, para crear efectos de impedimento físicos, empleando la decepción, engaño, falsificación y otras técnicas similares. Utiliza una fuente de información del adversario para nuestros propósitos, para crear efectos de engaño en el ciberespacio, no aparentes inmediatamente. La red del blanco, puede parecer que opera con normalidad hasta que efectos secundarios o terciarios, incluyendo efectos físicos, revelan la evidencia de la orden lógica del primer efecto.

c. Contramedidas en el ciberespacio.

Se entiende a aquellas formas de la ciencia militar que, mediante el empleo de mecanismos o técnicas, tienen como objetivo el deterioro de la actividad operacional del enemigo. En el ciberespacio, el termino aplica a cualquier acción de OC que se ajusta a la descripción del término, sin importar el dónde la contramedida es tomada. Así como en los dominios físicos, las acciones de contramedidas pueden ser internas o externas al terreno que se defiende, y pueden ser utilizadas de manera preventiva o reactiva. Las contramedidas internas, son acciones de defensa del ciberespacio, tomadas como parte de una misión de OCD-MDI. Las contramedidas externas, que pueden ser parte de una misión OCD-AR o OOC son empleadas más allá de las fronteras del ciberespacio del Comando Conjunto, en contra de una actividad maliciosa especifica. En apoyo de una misión OOC, puede haber acciones de ataque en el ciberespacio que engañen o nieguen la efectividad de los sensores o defensas del adversario. Como parte de una misión ODC-AR, ellas pueden ser utilizadas para identificar la fuente de la amenaza y/o el uso no intrusivo o técnica mínimamente intrusiva de para interdictar o mitigar las amenazas. Las contramedidas defensivas externas, son normalmente no destructivas/ no letales por naturaleza, impactan solamente en actividades maliciosas, pero no en los sistemas

asociados de la amenaza y termina cuando la amenaza se detiene. Todas las contramedidas externas, están sujetas a la misma sincronización, lineamientos legales y políticos, como cualquiera de las otras misiones OOC o ODC-RA.

AUTORIDAD, ROLES Y RESPONSABILIDADES.

La autoridad para la planificación ejecución de Operaciones militares en el ciberespacio está establecida dentro de las políticas emitidas por el Ministerio de Defensa, así como en las órdenes recibidas que autorizan al Comando de Ciberdefensa a la ejecución de estas operaciones.

a. Bajo la autoridad del Ministerio de Defensa, el Comando Conjunto emplea las capacidades en el ciberespacio para moldearlo y proveer opciones integradas (ofensivas y defensivas) para la defensa de la nación.

b. Mediante acuerdo ministerial No 281, Art 1, publicado en la O.G.M. No 188 del 24 de septiembre del 2014, el Ministro de Defensa Nacional, dio paso a la creación del Sistema de Ciberdefensa del Ministerio de Defensa Nacional, como el mecanismo de articulación de las instancias permanentes y de conformación que a fin de coordinar e implementar las políticas y estrategias de Ciberdefensa.

c. El Art 2; del mencionado acuerdo establece: “La Ciberdefensa o defensa cibernética, es el conjunto de políticas e instrumentos articulados a la protección y defensa de la infraestructura crítica e información estratégica del Estado. La rectoría del sistema lo ejerce el Ministerio de Defensa Nacional. La coordinación está a cargo del Comité de Ciberdefensa que tendrá como finalidad formular políticas de la Ciberdefensa”.

1. Autoridades.

El sistema de Ciberdefensa está conformado de la siguiente forma:

Tabla 2

Conformación del Sistema de Ciberdefensa, según Acuerdo Ministerial 281, Art 1, del 24 de septiembre de 2014

Sistema de Ciberdefensa		
Nivel	Responsable	Funciones
Político Estratégico	• MIDENA • Comité de Ciberdefensa • Dirección de Ciberdefensa	• Formulación del Concepto político estratégico de la Ciberdefensa • Relacionamiento regional e internacional
Estratégico Militar	• CC.FF.AA.	• Formulación de la estrategia militar de Ciberdefensa. • Formulación de planes militares
Operacional	• Comando de Ciberdefensa	• Planificación y ejecución de las OC.

Roles y responsabilidades

a. Del Ministro de Defensa.

Orienta y dirige las operaciones militares, de inteligencia y ordinarias de las FFAA en el ciberespacio. Por intermedio del Comité de Ciberdefensa, es responsable por:

(1) Articular con los diferentes organismos internos, el desarrollo de capacidades para prevenir, detectar y defender las posibles amenazas que provienen del ciberespacio y del espectro radioeléctrico que afecten significativamente al país.

(2) Diseñar la concepción político-estratégica de Ciberdefensa en concordancia con la Agenda Política de la Defensa.

(3) Monitorear y evaluar la implementación de las políticas de Ciberdefensa, así como del adecuado funcionamiento de los sistemas de información, comunicación e inteligencia relativos al ciberespacio.

(4) Promover la concepción política estratégica de Ciberdefensa a nivel nacional.

(5) Coordinar con las instancias correspondientes, el diseño de políticas públicas a nivel nacional en el ámbito de su competencia.

(6) Coordinar con las instancias competentes, el diseño de políticas a nivel regional que permitan la interacción de los órganos directivos y operativos de los Estados en el ámbito de Ciberdefensa.

(7) Promover iniciativas de capacitación y formación en el ámbito de Ciberdefensa.

(8) Las demás que, dentro de su ámbito de acción, le corresponde a la máxima autoridad del Ministerio de Defensa Nacional.

b. Del Comando Conjunto

Como responsable general, asesora al Presidente y al Ministro de Defensa sobre las políticas operacionales, responsabilidades y programas.

(1) Asesora al Ministro de Defensa, en la implementación de las respuestas operacionales a las amenazas en el ciberespacio.

(2) Traslada los lineamientos del Ministro de Defensa en órdenes.

(3) Se asegura que los planes y operaciones en el ciberespacio son compatibles con los otros planes y operaciones militares.

c. De los comandantes de fuerza.

Son quienes proporcionan la administración apropiada y el apoyo a las fuerzas asignadas al Comando de Ciberdefensa.

(1) Proporcionar el apoyo y la administración adecuada a las fuerzas del ciberespacio, así como a las fuerzas asignadas o agregadas a los comandos operacionales.

(2) Entrenar y equipar a las fuerzas del ciberespacio y desarrollar capacidades en el ciberespacio para el despliegue y apoyo a los comandos operacionales.

(3) Cumplir con las directrices emitidas por el Comando de Ciberdefensa para la seguridad, operación y defensa de sus segmentos respectivos del ciberespacio dentro del SICC.

(4) Coordinar con el Comando de Ciberdefensa para priorizar los requerimientos y las capacidades de la fuerza para las misiones en el ciberespacio.

d. Del Comando de Ciberdefensa

El estatuto de gestión por proceso del Comando Conjunto, establece la siguiente misión para el Comando de Ciberdefensa: “Efectuar operaciones de defensa y exploración en el Ciberespacio en forma permanente, protegiendo la infraestructura crítica tecnológica de Fuerzas Armadas y otras asignadas, degradando o neutralizando la infraestructura crítica tecnológica del adversario con orden, a fin de contribuir al cumplimiento de la misión del Comando Conjunto de las Fuerzas Armadas”.

(1) Como la autoridad de coordinación para las OC, planifica, coordina, integra, sincroniza y conduce actividades para:

(a) Dirigir la seguridad, las operaciones y la defensa del SICC.

(b) Estar preparado y cuando sea requerido, conducir OC militares externas al SICC,

incluyendo el ciberespacio gris y rojo, en apoyo a los objetivos nacionales.

(2) En concordancia con las leyes y políticas nacionales, prevenir los conflictos que puedan presentarse como consecuencia de la explotación del ciberespacio y delos ataques en el ciberespacio.

(3) Para las OC que requieren acciones y efectos en múltiples áreas de operaciones geográficas, el comando de Ciberdefensa es el comandando apoyado.

(4) Orientar a los sensores de la CI y los sensores del SICC como sea apropiado, para establecer y permitir una alerta situacional comprensiva sobre los ciberespacios gris y rojos en apoyo a la misión asignada.

(5) Coordinar con la comunidad de Inteligencia (CI), Comandos Operacionales, Fuerzas y otras organizaciones gubernamentales para facilitar el desarrollo y mejorar el acceso al ciberespacio para apoyar la planificación y las operaciones.

(6) Es el responsable de la representación militar ante los organismos gubernamentales, entidades comerciales y organizaciones internacionales en asuntos relacionados con el ciberespacio.

e. De los comandantes operacionales

Son responsables de asegurar, operar y defender los segmentos tácticos del SICC, dentro de sus comandos operacionales y áreas de responsabilidad.

(1) Integrar las OC dentro de sus planes; integrar las capacidades del ciberespacio con las operaciones militares de ser requerido; y trabajar estrechamente con la FC, el Comando de Ciberdefensa y otros organismos gubernamentales para la creación de capacidades totalmente integradas.

(2) En coordinación con el Comando de Ciberdefensa, articular los esfuerzos para la planificación de las CO, designar los efectos deseados de las CO, y determinar el timing (secuencia) y el tempo (ritmo) para la conducción de las OC en apoyo a sus misiones.

f. Del Secretario de Inteligencia Nacional

Proporcionar inteligencia militar oportuna, objetiva y relevante a las unidades de combate, planificadores de la defensa y a los planificadores de la política de seguridad nacional.

(1) Conducir el análisis de todas las fuentes en apoyo a las OC, incluyendo la contribución para el desarrollo de los productos de la preparación de inteligencia del Ambiente Operacional / Área de Operaciones (AO)[73] relacionado con las OC.

(2) Desarrollar y mantener su Tecnología de Información (TI)[74] de forma consistente con la arquitectura desarrollada por el SICC, manteniendo los estándares de Ciberseguridad y la planificación, recursos, adquisiciones, implementación y mantenimiento de las especificaciones técnicas en concordancia con la política gubernamental y la priorización de recursos.

[73] Ambiente Operacional / Área de Operaciones : AO
[74] Tecnología de Información :TI

g. Consideraciones legales.

El Comando Conjunto conduce OC en concordancia con la ley nacional, y en concordancia con las leyes y tratados internacionales, así como políticas relevantes emitidas por el Ministerio de Defensa.

(1) El Comando Conjunto conduce las OC dentro de la ley nacional y en concordancia con las leyes internacionales y las políticas emitidas por el Ministerio de Defensa. Las leyes que restringen las acciones militares dentro del territorio nacional, son aplicables al ciberespacio. Por lo tanto las fuerzas del ciberespacio que operan fuera del SICC, cuando están autorizadas debidamente, normalmente se limitan a la operación en el ciberespacio gris o en el rojo, de acuerdo a las reglas de enfrentamiento elaboradas por la autoridad militar competente.

(2) Aplicación de las leyes de la guerra. Los miembros de las FF. AA, deben cumplir con las leyes durante los conflictos armados y en todas las operaciones militares. Estas leyes están inmersas, dentro de la ley internacional que permite la conducción de hostilidades armadas para proteger los intereses

nacionales o sus ciudadanos; incluyendo los tratados internacionales de los cuales nuestro país es signatario. Las leyes de la guerra se fundamentan en los principios de necesidad militar, proporcionalidad, distinción (discriminación) y de evitar el sufrimiento innecesario, todo los cual puede ser aplicado en las OC.

Conclusiones Parciales

Las OC comprenden las operaciones militares, nacionales y ordinarias que se desarrollan en el ciberespacio. Las operaciones militares en el ciberespacio están organizadas en misiones ejecutadas mediante una combinación de acciones específicas.

Muchos aspectos de las operaciones conjuntas se basan en parte en la utilización del ciberespacio, dominio existente dentro del Ambiente Informacional (AI)[75], que consiste de la red interdependiente de la Tecnología de Información (TI)[76], infraestructura e información residente (base de datos). Incluye el internet, redes de telecomunicaciones, sistemas de computación, procesadores y controladores. Las Operaciones en el Ciberespacio (OC)[77], consisten en el empleo de las capacidades del ciberespacio, con el propósito primario de alcanzar objetivos en y mediante el ciberespacio.

[75] AI: Ambiente Informacional/ Área de Interés
[76] TI: Tecnología de Información
[77] OC: Operaciones en el Ciberespacio

c) Analizar la planificación por capacidades del Comando Conjunto de las FF.AA.

Introducción

La planificación basada en capacidades aplicada por Fuerzas Armadas ecuatorianas proporciona un fundamento más racional para la toma de decisiones sobre la modernización del material existente, adquisiciones futuras y el sostenimiento operacional, a la vez que ofrece soluciones integrales, para afrontar con éxito los actuales y potenciales escenarios de conflicto. El objetivo general del Plan de Capacidades es enfocar las operaciones militares hacia la acción conjunta para conseguir la máxima eficacia en los resultados, evitando las necesidades y soluciones aisladas y no orientadas a la consecución de los objetivos estratégicos de FF.AA. Considerando que capacidad se define como la aptitud o suficiencia específica que le permite a una organización cumplir con su misión básica y sus funciones, las capacidades que deben tener las Fuerzas Armadas ecuatorianas han sido determinadas por capacidades estratégicas y capacidades específicas, las cuales les permitirán cumplir con la misión constitucional y con las misiones subsidiarias asignadas.[78] (Ardieta, 2013)

[78] Plan de Gestión Institucional de FF. AA 2010 - 2021

Conocimiento del Hecho

El nuevo diseño de Fuerzas, debe responder al desarrollo de capacidades para el empleo conjunto de las Fuerzas Armadas, para enfrentar con éxitos las amenazas, riesgos y desafíos del Estado, en los actuales y futuros escenarios estratégicos de seguridad y defensa, así como en las amenazas emergentes.

Las Capacidades Estratégicas Conjuntas de Fuerzas Armadas son:

a) Mando y Control.
b) Vigilancia, Reconocimiento e Inteligencia.
c) Maniobra
d) Despliegue y Movilidad.
e) Supervivencia y Protección.
f) Sostenimiento Logístico.
g) Apoyo a la Gestión del Estado.

El nuevo sistema de planeamiento contempla todos los aspectos inherentes a cada requerimiento operativo, desde que tal requerimiento se concibe hasta que deje de ser útil. Evita centrarse únicamente en la adquisición del sistema principal y dejar partes esenciales de su “ciclo de vida” para otros momentos presupuestarios.

No persigue solo determinar las capacidades o medios necesarios para un determinado tipo de conflicto o para cumplir una misión

específica, sino que es mucho más general y va dirigido hacia la obtención de capacidades que permitan abarcar un amplio espectro de amenazas y riesgos.

Por la experiencia vivida en 1995 y la incidencia del nuevo proceso de planificación a nivel mundial, a partir del año 2006 se inicia el análisis y propuesta para implementar la planificación por capacidades a nivel Fuerzas Armadas.

Los sistemas de Planeamiento Militar tradicionales, empleados en varios países, tenían su fundamento en el conocimiento más o menos exacto de la "Amenaza" y de sus más probables "Líneas de Acción", ajustándose a la situación estratégica del momento y traduciéndose en el análisis de un escaso número de escenarios; esto permitía desde el primer momento, una fácil identificación de las capacidades o medios necesarios para combatir o anular la amenaza predefinida. En definitiva, los trabajos, como norma general, se orientaban al apoyo en la toma de decisiones relacionadas con la renovación de los sistemas existentes o la adquisición de unos nuevos, ofrecidos por las nuevas tecnologías.[79]

El nuevo sistema denominado "Planeamiento por Capacidades", ha sido adoptado también por los países líderes en el ámbito de la Defensa, tales como Estados Unidos, España, Colombia, entre otros.

[79] Sistema de Planeamiento por Capacidades del MIDENA 2016

El Sistema de Planeamiento por Capacidades determina las capacidades conjuntas y especificas respecto a los escenarios, amenazas, riesgos y misiones, su condición y requerimientos que permitan fortalecerlas evitando las necesidades y soluciones aisladas y no orientadas a la consecución de los objetivos propuestos.

La determinación de las capacidades proporciona un fundamento más eficiente para la toma de decisiones sobre la modernización del material existente, adquisiciones futuras, adaptación y el sostenimiento operacional, a la vez ofrece soluciones integrales, para accionar con éxito en los actuales y potenciales escenarios.

Análisis

La incertidumbre en los escenarios actuales se presenta como factor principal que obliga a enfrentar amenazas de carácter sutil, multipolar e indefinido, en donde la inteligencia y la innovación resultarán elementos fundamentales para determinar las soluciones encaminadas a combatirla o anularla. Es precisamente la indefinición lo que obliga a los órganos de planeamiento a efectuar un esfuerzo de imaginación y desarrollar este de forma más general, orientado a contrarrestar “lo que puede ser capaz de hacer nuestra amenaza” (el CÓMO), en lugar de “contra quién y en dónde debemos enfrentarnos” (el QUIÉN y el DÓNDE).

En el nivel político - estratégico a través del Ministerio de Defensa quien emite la Agenda Política de la Defensa, el Plan Estratégico Institucional de la Defensa, Agenda de investigación, desarrollo tecnológico e innovación; y la Directiva de Defensa Militar la misma que en su contenido determina los objetivos a alcanzar, plasmados en el Diseño de Fuerza deseado para las Fuerzas Armadas estableciendo líneas generales de actuación y directrices para el Planeamiento Militar, factores que condicionan el proceso, valoración de la situación estratégica y la coyuntura económica, la autorización al Comando Conjunto para la determinación y valoración de los requerimientos operacionales de las Fuerzas así como la consideración de los compromisos internacionales.[80]

En el nivel estratégico - militar a través del Comando Conjunto quien emite el Concepto Estratégico de Fuerzas Armadas el mismo que detalla los escenarios de empleo identificando las amenazas y riesgos, organización de las Fuerzas, nivel de exigencia, situación actual de las capacidades estratégicas, direccionamiento para el desarrollo de capacidades, capacidad operativa deseada, empleo conjunto y coordinado y cumplimiento de los derechos humanos y D.I.H, en el accionar de las Fuerzas Armadas. La Directiva de Gestión Institucional y de Planeamiento Militar establecerá directrices para la

[80] Sistema de Planeamiento por capacidades del MIDENA 2016

elaboración de los Planes de Gestión y Planes militares respectivamente.[81]

Conclusiones Parciales

Una capacidad militar no es únicamente un arma o un sistema de armas, sino que es algo más, es un conjunto de factores, unos más críticos que otros, pero que en definitiva son igualmente importantes para la consecución del efecto deseado.

El Planeamiento por Capacidades permite el diseño de la Fuerza y la determinación de los medios y recursos necesarios basados en los escenarios, misiones y estrategias establecidas, alcanzando las capacidades militares que permitan cumplir los objetivos dispuestos desde el nivel político.

El Planeamiento por Capacidades es un proceso que se establece para un periodo de cuatro años coincidente con el ciclo de gobierno, debiendo ser revisado anualmente. Se trata de un proceso continuo que tiene la flexibilidad suficiente para reaccionar ante nuevos requerimientos y retos de las Fuerzas Armadas.

El Planeamiento por Capacidades se basa en los lineamientos establecidos en el marco legal, en el nivel político a través del

[81] Sistema de Planeamiento por capacidades del MIDENA 2016

Consejo de Seguridad Pública y del Estado quien emite el Plan Nacional de Seguridad Integral.

d) Determinar las amenazas y riesgos existentes para el Comando de Ciberdefensa.

Introducción

El mundo vive una época de incertidumbre marcada fundamentalmente por eventos violentos, que amenazan a la defensa y seguridad de los Estados de manera permanente.

En este sentido, la comunidad internacional ha conceptualizado las amenazas y riesgos de acuerdo con el ámbito en el que se desenvuelven; tal es el caso de las Naciones Unidas, que define como amenazas emergentes a "...cualquier suceso o proceso que cause muertes en gran escala o una reducción masiva en las oportunidades de vida y que socave el papel del Estado como unidad básica del sistema internacional, todo esto conlleva una amenaza a la seguridad internacional". El mismo organismo considera seis grupos de amenazas: las amenazas económicas y sociales (la pobreza, enfermedades infecciosas y la degradación ambiental); los conflictos entre Estados; los conflictos internos (la guerra civil, el genocidio y otras atrocidades en gran escala); las armas nucleares, radiológicas, químicas y biológicas; el terrorismo; y, la delincuencia organizada transnacional. (Defensa, 2018)

La multiplicidad de potenciales atacantes incrementa los riesgos y amenazas que pueden poner en graves dificultades los servicios prestados por las Administraciones Públicas, las infraestructuras Críticas o las actividades de las empresas y ciudadanos. Además, existen evidencias de que determinados países disponen de capacidades militares y de inteligencia para realizar ciberataques que ponen en riesgo la Seguridad Nacional.[82]

Conocimiento del Hecho

América Latina, es considerada una zona de paz por la ausencia de conflictos armados interestatales, debido a la adopción de la diplomacia como vía para su solución; sin embargo, no se descarta el empleo del poder militar debido a la confrontación de intereses y al desbalance de las capacidades estratégicas militares en la región.

Por consiguiente, debido a la dinámica permanente de los escenarios geopolíticos, las amenazas varían constantemente con el aparecimiento de nuevos actores y desafíos asociados a factores políticos, sociales, económicos, ambientales y estructurales del Estado, por lo que es necesario mantener un monitoreo permanente de estos elementos, para diseñar medidas preventivas que reduzcan sus potenciales efectos.

[82] Estrategias de Ciberseguridad Nacional 2013 España

Partiendo del marco de la Carta de las Naciones Unidas, que "reconoce a todo Estado el derecho inmanente de legítima defensa" y considerando que es deber primordial del Estado garantizar y defender la soberanía nacional, la integridad territorial, la población y sus recursos naturales, se caracteriza como una amenaza a la agresión armada externa perpetrada por las Fuerzas Armadas de otro Estado[83].

La defensa nacional permite mantener el control sobre la incidencia de amenazas y riesgos, aportando así al incremento en los niveles de seguridad del país. Ante las amenazas que enfrenta el Ecuador, las Fuerzas Armadas cuentan con el nivel de alistamiento adecuado para enfrentarlas: con talento humano idóneo y competente, entrenado sobre la base de una doctrina actualizada, con un orgánico estructural y numérico, material y medios que permiten cumplir la misión fundamental y misiones complementarias. Paralelamente, el accionar de las Fuerzas Armadas cuenta con el apoyo de los servicios brindados por los institutos adscritos a la defensa para la ejecución de las operaciones militares. El sector Defensa impulsa la coordinación interinstitucional de la Ciberdefensa en el marco de la seguridad cibernética nacional y posee una capacidad considerable para defender la infraestructura crítica digital de las Fuerzas Armadas.[84]

[83] Agenda Política de la Defensa 2018
[84] Agenda Política de la Defensa 2014-2017

El Estado al haber definido sus intereses vitales y estratégicos en la agenda política de la defensa, requiere garantizar la vigencia de los mismos; por tanto, al existir amenazas y riesgos que inciden en la consecución de estos, debe estar en condiciones de protegerlos. Es entonces cuando la defensa se constituye en el instrumento para el empleo de la fuerza ante la amenaza externa que atenta contra estos intereses. (Defensa, 2018)

La defensa nacional constituye un componente esencial de la seguridad nacional que, articulada con la seguridad pública, la política exterior, el apoyo del sistema de inteligencia nacional, garantiza la defensa de la soberanía e integridad territorial y la protección de la población y de los recursos; con los mecanismos de cooperación internacional contribuye a crear un entorno nacional y regional estable y seguro.

Análisis

La Ciberseguridad, es una necesidad de nuestra sociedad y de nuestro modelo económico. Dada la influencia de los Sistemas de Información y Telecomunicaciones en la economía y en los servicios públicos, la estabilidad y prosperidad de Ecuador depende en buena medida de la seguridad y confiabilidad del ciberespacio, cualidades que pueden verse comprometidas por causas técnicas, fenómenos naturales o agresiones deliberadas.

La tecnología se ha convertido en un factor indispensable para el funcionamiento y futuro desarrollo de nuestra sociedad. Gracias a ella, hoy en día podemos acceder a grandes cantidades de información en tiempo y forma, independientemente de su ubicación física, desapareciendo así las barreras y fronteras tradicionales, lo que ha dado paso a la denominada Sociedad de la Información.

Del mismo modo, las Fuerzas Armadas tienen una alta dependencia de las Tecnologías de la Información y las Comunicaciones (TIC)[85], ya que constituyen un pilar básico para poder llevar a cabo las operaciones militares. Sin embargo, este nuevo dominio donde operan estas tecnologías y que se ha venido a denominar el «Ciberespacio», está lleno de un gran número de amenazas que ponen en peligro el éxito de las operaciones militares, así como a las personas que las llevan a cabo.

Tradicionalmente, la seguridad en las TIC en el ámbito militar se ha centrado en la protección de las comunicaciones, aunque hoy en día el uso masivo de sistemas de información hace necesario disponer de una perspectiva más amplia y abordar el problema de una forma integral. De este modo surge el concepto de Seguridad de Gestión de la Información, (SGSI)[86] que se basa en medidas de protección estáticas para los sistemas. (Cornaglia, 2017)

[85] TIC´S: Tecnologías de la Información y las Comunicaciones
[86] SGSI: Sistema de Gestión de la Seguridad de la Información

Sin embargo, la evolución de la amenaza en los sistemas de información, requiere adoptar un conjunto completo de medidas de seguridad que incluyan tanto las de carácter preventivo, como aquellas otras que aborden el carácter cambiante y asimétrico de la ciberamenaza, acción que debe llevar implícita una perspectiva dinámica que complemente la aproximación estática tradicional citada (SGSI).[87] Esta aproximación dinámica, se engloba hoy en el término denominado “Ciberdefensa”, que se puede definir como un conjunto de recursos, actividades, tácticas, técnicas y procedimientos para preservar la seguridad de los sistemas y la información que manejan, así como permitir la explotación y respuesta sobre los sistemas adversarios, para garantizar el libre acceso al ciberespacio y permitir el desarrollo eficaz de las operaciones militares y el uso eficiente de los recursos. (Zea, 2013)

Se puede considerar como amenaza a "aquel fenómeno o proceso natural, causado por el ser humano que puede poner en peligro a una persona, grupo, comunidad, estado o la comunidad internacional".[88]

De acuerdo, a lo que enuncia (Pérez, 2018), todos los componentes que estructuran el ciberespacio y sus diferentes amenazas se constituyen en riesgos latentes para los individuos y los

[87] SGSI: Sistema de Gestión de la Seguridad de la Información
[88] Concepto de Amenaza del Manual de Defensa Interna MIP-10-01-2010, CEDE

estados, sobre todo las grandes naciones que dependen en un 80% de su manejo tecnológico a través de redes.

Las amenazas cibernéticas tienen una connotación diferente a la de otras amenazas a la seguridad del Estado; dado que éstas pueden tener diferentes objetivos, pueden ser realizadas por diferentes tipos de actores como el crimen organizado, terroristas u otros Estados, su costo es mínimo y su trazabilidad es complicada.

Durante los últimos años, las naciones se han visto obligadas a actualizar sus Estrategias Nacionales de Seguridad y Defensa hacia un nuevo escenario que es el CIBERESPACIO debido a las diversas razones que han producido un incremento de Amenazas y Riesgos[89]:

La tecnología y el espectro electromagnético, es la base del ciberespacio, y también sobre la que se apoyan las principales amenazas de éste y en éste. Un enfoque aséptico tecnológico del ciberespacio da cabida a las dos visiones previas, tanto la pesimista como la optimista. Tan cierto es que las amenazas crecen, se especializan y sofistican sus métodos de manera continua, como que las ventajas que aporta el ciberespacio, y las herramientas de defensa de las que se dispone, y no sólo tecnológicas, permiten

[89] "AMENAZAS INFORMÁTICAS EN LA WEB 3.0": Guía para aprender a identificar y prevenir los riesgos a los que usted y su familia, se exponen, al navegar en Internet, Félix A. Reyes G. y Carlos Andrés Lugo González, (Spanish Edition) Kindle Edition, 15 de Agosto 2018

asegurar que este es un medio irrenunciable que establece un nuevo paradigma de cohesión mundial.

Se ha visto necesario que el Comando de Ciberdefensa (COCIBER), considere dentro de sus lineamientos ciertas actividades esenciales de las operaciones del ciberespacio

a. **Las Operaciones en el Ciberespacio OC[90]**

Consisten en el empleo de capacidades en el ciberespacio donde el propósito primario es alcanzar objetivos en o dentro del ciberespacio. Las OC comprenden la inteligencia militar, inteligencia nacional y las actividades ordinarias del Comando Conjunto y del Ministerio de Defensa, dentro y a través del ciberespacio. A pesar de que los comandantes deben ser advertidos sobre el impacto potencial de las operaciones que desarrolla el Comando de Ciberdefensa sobre sus operaciones, el componente militar de las OC, es el único que debe ser guiado por esta doctrina y es el focus para esta publicación. Las operaciones militares en el ciberespacio están organizadas en misiones ejecutadas mediante una combinación de acciones específicas que contribuyen a la consecución de los objetivos del comandante.

[90] Operaciones en el Ciberespacio: OC

b. Actividades habilitadas para el ciberespacio.

La mayoría de las acciones del ciberespacio utilizan el ciberespacio para facilitar otros tipos de actividades, que emplean las capacidades del ciberespacio para completar otras tareas que no son parte de las tres misiones de las Operaciones en el Ciberespacio: Operaciones ofensivas en el Ciberespacio (OOC)[91], Operaciones defensivas en el Ciberespacio (ODC)[92] y las operaciones del Comando Conjunto. Esa utilización incluye acciones como la operación de un sistema de comando y control (C2)[93] o de un sistema logístico, él envió de un email para apoyar un objetivo de información, el uso del internet para completar un curso de entrenamiento online, o para desarrollar un briefing. Otros usuarios, que pueden ser usuarios no autorizados de *network,* personal del Comando Conjunto que no necesita una autorización especial para utilizar las capacidades del ciberespacio, etc.

Es por tanto a través del ciberespacio que la mayoría de las vulnerabilidades del sistema del Comando Conjunto, pueden estar expuestas y ser explotadas por nuestros adversarios. El desafío es entrenar a todos los usuarios del Comando

[91] Operaciones ofensivas en el ciberespacio: OOC
[92] Operaciones defensivas en el ciberespacio: ODC
[93] Comando y Control: C2

Conjunto para comprender el significado de las amenazas del ciberespacio, y a reconocer las tácticas de la amenaza para que el uso del ciberespacio no genere un riesgo innecesario a las operaciones. La protección del ciberespacio del Comando Conjunto mediante el establecimiento de una cultura de prevención de las vulnerabilidades, particularmente mediante políticas, prácticas y entrenamiento, es crítico para el éxito de todos los tipos de operaciones permitidas en el ciberespacio.

c. Defensa del Ciberespacio que no pertenece al Comando Conjunto.

Mientras que las ODC generalmente se enfocan en la defensa del SICC, el cual incluye el ciberespacio del Comando Conjunto, las fuerzas militares del ciberespacio deben estar en condiciones de defender otra porción del ciberespacio azul cuando sean requeridas. Las operaciones del SICC, se apoya en varios segmentos que no pertenecen al ciberespacio del Comando Conjunto, incluyendo el sector privado y otros socios comerciales.

La seguridad de este ciberespacio es responsabilidad de los propietarios de los recursos, que incluye otros ministerios y agencias gubernamentales, Debido a que el ciberespacio asociado con el Comando Conjunto es un banco conocido

para actividades maliciosas en el ciberespacio, la protección de las redes y sistemas que laboran en esta porción del ciberespacio puede ser un componente vital para asegurar el cumplimiento de la misión.

d. Operaciones de Inteligencia Nacional en y a través del Ciberespacio.

Las organizaciones del nivel nacional de inteligencia conducen actividades de inteligencia en, a través y sobre el ciberespacio en respuesta a las prioridades de inteligencia nacional. Esta inteligencia puede apoyar la planificación y preparación del comandante militar. A pesar de que las fuerzas del ciberespacio del Comando Conjunto, pueden obtener información táctica y operacional útil, mientras maniobran hacia y dentro el ciberespacio extranjero, al igual que todas las fuerzas conjuntas, ellas también dependen del apoyo de las fuentes de inteligencia militares y nacionales, tradicionales.

e. Operaciones ordinarias del Comando Conjunto en y a través del Ciberespacio.

Las operaciones normales que se ejecutan en y a través del ciberespacio se denominan “actividades permitidas en el

ciberespacio” que comprenden aquellas capacidades, distintas a las de inteligencia y de aplicación a las operaciones militares, funciones y acciones usadas para apoyar y sostener a las fuerzas y sus componentes. Esto incluye las funciones permitidas en el ciberespacio del ámbito civil y otras relacionadas con las finanzas y sostenimiento administrativo. Estas actividades deben ser conducidas dentro de las políticas establecidas por el Comando Conjunto y no se encuentran bajo la doctrina conjunta. A pesar de ello, pueden existir vulnerabilidades en las aplicaciones y mecanismos utilizados para la operación ordinaria del Comando Conjunto, y podrían ser explotadas de una manera que tenga impacto directo sobre las operaciones militares.

f. **Las funciones conjuntas y las operaciones del Ciberespacio**.

La publicación PC-3 “Operaciones Conjuntas”, describe las funciones conjuntas que son comunes a las operaciones conjuntas en todos los niveles de la guerra. Estas funciones conjuntas comprenden capacidades y actividades relacionadas y agrupadas que ayudan al comandante a integrar, sincronizar y dirigir las operaciones conjuntas. Esta sección presenta una descripción de como las capacidades para desarrollar operaciones militares en el ciberespacio

pueden facilitar dichas funciones en apoyo a todas las misiones del CFC y como las funciones en sí mismas son ejecutadas en el ciberespacio durante las OC.

g. Comando y Control (C2).

La discusión entre C2 y ciberespacio requiere distinguir entre la utilización de los sistemas del ciberespacio que implementan el C2 de las operaciones militares y el C2 de las fuerzas que ejecutan las OC. La primera, es una actividad permitida en el ciberespacio y la última será descrita en el Capítulo IV “Planificación, coordinación ejecución y evaluación” párrafo 5, “C2 de las fuerzas del ciberespacio”. El C2, incluye el ejercicio de autoridad y dirección por parte de los comandantes sobre las fuerzas asignadas o agregadas para el cumplimiento de su misión. El uso del ciberespacio como un medio para intercambiar comunicaciones es el método más común en los niveles estratégico y operacional de la guerra, y está incrementándose significativamente en el nivel táctico. Métodos de comunicación digitales han reemplazado a los métodos análogos, excepto en el nivel táctico, donde los métodos análogos de señales permanecen. Las comunicaciones analógicas, permanecerán indefinidamente en las operaciones tácticas por razones como la simplicidad, confiabilidad y seguridad. Sin embargo, los

sistemas militares de C2, funcionan mediante la trasmisión digital de información como parte del SICC. El ciberespacio proporciona autopistas para las comunicaciones, ayuda en la planificación y toma de decisiones, e inteligencia del ciberespacio relacionada que permite la toma de decisiones y su ejecución oportuna. Esto proporciona la comandante la ventaja de controlar el timing y el ritmo de las operaciones (tempo). El Ciberespacio ofrece una gama diversa y excepcional de circuitos para la emisión de órdenes y señales a las fuerzas y para aquellas fuerzas que dependen de la retransmisión de la información en su cadena de mando. Las órdenes militares se convierten a un formato digital, incluyendo voz y video, pueden viajar a través de los circuitos que los transmiten en todos los dominios físicos, incrementando la posibilidad de la deliberación oportuna. Sin embargo, la confianza del comandante sobre el sistema de C2 puede verse fácilmente comprometida cuando la seguridad del SICC se ve comprometida; por lo tanto, a mayor dependencia del comandante en el ciberespacio para ejecutar el C2, mayor preocupación debe ser puesta para incrementar la protección de los mecanismos del ciberespacio.

h. Inteligencia.

La comprensión del AO es fundamental para todas las operaciones conjuntas, incluidas las OC. La inteligencia puede ser derivada de la información obtenida durante las operaciones militares en el ciberespacio o de otras fuentes. Las operaciones de inteligencia en el ciberespacio no conducidas por un comandante militar son cubiertas en el párrafo 3, “Operaciones de Inteligencia Nacional, en y a través del ciberespacio”. El apoyo de todas las fuentes de inteligencia a las OC utiliza el mismo proceso de inteligencia utilizado en todas las operaciones militares, con atributos únicos necesarios para apoyar el planeamiento detallado de las OC, este proceso incluye:

(1) Planeamiento y dirección, incluyendo la identificación de las vulnerabilidades de los blancos, que permitan la planificación continua y dirección de las actividades de CI para protegernos contra el espionaje, sabotaje, y ataque en contra de los ciudadanos o facilidades del estado.

(2) Sensores de búsqueda con acceso a la información sobre el ciberespacio.

(3) Procesamiento y explotación de información recolectada, incluyendo la identificación de la utilidad sobre dicha información, en tiempo real.

(4) Análisis de la información y productos de inteligencia

(5) Diseminación e integración de la inteligencia relacionada con el ciberespacio y las operaciones.

(6) Evaluación y retroalimentación, indiferente de la efectividad y calidad de la inteligencia.

i. Fuegos.

Las capacidades de ataque en el ciberespacio crean fuegos en y a través del ciberespacio, y a menudo pueden ser empleadas con poca o ninguna destrucción física asociada. Sin embargo, la modificación o destrucción de computadores, que controlan los procesos físicos, pueden conducir a efectos cascada (incluyendo efectos colaterales) en los dominios físicos. Dependiendo de los objetivos del comandante, los fuegos en el ciberespacio pueden ser ofensivos o defensivos, o en apoyo. Al igual que todas las formas de fuegos, los fuegos en y a través del ciberespacio, deben ser incluidos en el proceso de planificación y ejecución conjunta, para facilitar

la sincronización y la unidad de esfuerzo, debiendo cumplir con todas las leyes de la guerra y las reglas de enfrentamiento. Los fuegos en y a través del ciberespacio, incluyen un número de tareas, acciones y procesos, incluyendo la designación de blancos, la coordinación, etc.

j. Movimiento y maniobra

El movimiento y maniobra incluye el despliegue de las fuerzas y las capacidades dentro del área de operaciones, y el posicionamiento dentro de esa área, para obtener una ventaja operacional en apoyo a los objetivos de la misión, incluyendo el acceso y/o el control del terreno clave. Las OC, facilitan la proyección de la fuerza sin la necesidad de establecer la presencia física en territorio enemigo. La maniobra en el ciberespacio del SICC u otro ciberespacio azul, incluye el posicionamiento de fuerzas, sensores, y defensas para asegurar de la mejor forma áreas en el ciberespacio o emplearse en acciones defensivas de ser requerido. La maniobra en los ciberespacios gris o rojo, es una acción de explotación del ciberespacio e incluye actividades como ganar acceso a links y nodos del adversario, enemigo o intermediario, y dar forma al ciberespacio para apoyar acciones futuras. La habilidad para acceder o aun controlar dicho terreno puede cambiar el entorno de un combate. Un

factor significativo en la maniobrabilidad en el ciberespacio es ganar y mantener el acceso lógico al ambiente. Esta capacidad para maniobrar y proporcionar alcance operacional puede ser perdida en cualquier tiempo si la configuración de los nodos relevantes en el ciberespacio es modificada. La omnipresente naturaleza del ciberespacio, crea otras consideraciones mayores, ya que esto permite que el adversario o enemigo establezca puntos clave de presencia, fuera del área de operaciones física, en terceros países, en áreas protegidas o dentro del propio territorio nacional. Adicionalmente, los adversarios o enemigos pueden conducir OC desde conexiones de redes físicas dentro del país, en terceros países, en donde la capacidad de maniobra del Comando Conjunto se ve limitada por restricciones legales o políticas, y la dependencia existente para generar coordinaciones con otros organismos del estado. Otro componente de la maniobra en el ciberespacio es la habilidad para mover información a un lugar o proceso en donde existe la máxima utilidad militar, incluyendo el movimiento de información disponible a mano a un lugar a una posición o proceso seguro.

k. Sostenimiento.

El sostenimiento, es la provisión de servicios logísticos y de personal para mantener la operación hasta el cumplimiento de la misión y el redespliegue de la fuerza. Desde la perspectiva de las actividades permitidas en el ciberespacio, el Comando Conjunto confía en un SICC y segmentos de redes comerciales para coordinar el sostenimiento de la fuerza.

Los avances rápidos en las TI, requieren del desarrollo, fortalecimiento y sostenimiento de las capacidades del ciberespacio que se adapten a un AO cambiante. Por ejemplo: mecanismos móviles, seguros, inalámbricos, proporcionan anonimidad para los usuarios adversarios del internet; un adversario puede actualizar o cambiar los sistemas operativos, o pueden transicionar para utilizar máquinas virtuales más seguras dentro de su arquitectura de red. Las fuerzas conjuntas deben tener la capacidad para adaptarse incorporando rápidamente nuevas capacidades en su arsenal del ciberespacio. Adicionalmente, deben tener la capacidad de actualizar su propio ciberespacio para equilibrar el desarrollo de esas nuevas tecnologías, pero se debe considerar que cualquier modificación debe ser cuidadosamente realizada para prevenir la creación de vulnerabilidades en la arquitectura del SICC.

I. Protección.

La protección del SICC y otros ciberespacios nacionales críticos incluye la sincronización continua y la integración de la seguridad en el ciberespacio y, cuando sean requeridas, acciones defensivas. La protección de los medios del ciberespacio es complicada debido a su conectividad lógica, que facilita al enemigo la creación de efectos de cascada múltiples, que no pueden ser restringidos por la geografía física o fronteras civiles o militares. Las capacidades del ciberespacio que requieren protección, incluyen no solamente la infraestructura (computadores, cables, antenas, y equipamiento de conexión y ruta) sino también partes del EEM (frecuencias, enlaces satelitales, celulares e inalámbricos) y los contenidos (bases de datos y aplicaciones), sobre las cuales se basan las operaciones militares. La clave en la protección del ciberespacio es un control positivo de todas las conexiones directas entre el SICC y la internet y otra porción pública del ciberespacio, así como la habilidad para monitorear, detectar y prevenir el acceso de tráfico malicioso en la red y la ex filtración no autorizada de información a través de dichas conexiones.

La protección del ciberespacio azul utiliza una combinación de capacidades defensivas y de seguridad del ciberespacio. Debido a la velocidad de los efectos y el número de los elementos en el ciberespacio, los procedimientos automáticos de defensa del ciberespacio, verificar las configuraciones y descubrir las vulnerabilidades de la red, a menudo proporciona una mejor oportunidad de éxito inicial en contra de un agresor que sus equivalentes manuales.

La protección del ciberespacio requiere de la adherencia estricta a las contramedidas previstas en las operaciones de seguridad, ya que dichas operaciones pueden ser amenazadas si son descubiertas en anticipación a sus efectos. Las habilidades para evitar la detección son fundamentales en las misiones externas y por lo tanto esenciales para las OC conjuntas.

m. Información.

La función de información, incluye la administración y aplicación de la información y su integración deliberada con las otras funciones conjuntas, para influenciar las percepciones delos actores relevantes, su comportamiento y/o su acción o inacción y el apoyo a la toma de decisiones humana o automática. La función de información ayuda al

comandante y su *staff* a entender y apalancar la naturaleza omnipresente de la información, su uso militar, y su aplicación durante todas las operaciones militares. Esta función proporciona al CFC la habilidad de integrar la generación y preservación de la información propia mientras que apalanca o sustenta los aspectos informacionales inherentes a todas las actividades militares para alcanzar los objetivos del comandante y el estado final deseado. Esta función de la fuerza conjunta apoya las acciones para alcanzar los objetivos dentro del ambiente informacional y operacional. Dado que el objetivo o propósito de las OC es alcanzar objetivos dentro del ciberespacio y el ciberespacio está totalmente contenido dentro del ambiente informacional, es importante comprender su relacionamiento con la función conjunta de información.

Conclusiones Parciales

Las amenazas globales tienen una connotación transnacional que podría afectar a la defensa y seguridad de los Estados. Entre otras, podemos señalar: el terrorismo, narcotráfico y sus delitos conexos, crimen organizado, ciberataques, exploración y explotación ilegal de los recursos marítimos, delincuencia organizada transnacional.

El Estado ecuatoriano concibe intereses nacionales vitales y estratégicos para garantizar la soberanía, propender al desarrollo nacional y alcanzar el bienestar de sus habitantes; por consiguiente,

tiene la responsabilidad de proteger su territorio, población y recursos frente a cualquier amenaza que atente contra sus intereses.

Para efectos de la Política de Defensa Nacional y en concordancia con lo señalado en la Declaración sobre Seguridad en las Américas, se conceptualiza a la amenaza como fenómenos, elementos o condiciones de naturaleza antrópica, caracterizada por su capacidad, motivación e intencionalidad de atentar contra los intereses vitales o estratégicos del Estado. (Defensa M. d., 2018)

Los riesgos son considerados como condición interna o externa generada por situaciones de origen natural o antrópico que pudieran afectar a la seguridad y defensa del Estado; su posibilidad de ocurrencia es incierta. En caso de no ser identificados oportunamente o no implementar acciones preventivas podrían traducirse en manifestaciones de peligro. Los riesgos causados por el hombre pueden convertirse en amenazas una vez que se identifique su motivación, capacidad e intención.

Los flujos migratorios irregulares, causados por la inseguridad social y económica en el lugar de origen de la población afectada, como consecuencia del accionar de factores naturales o antrópicos, obliga al Estado a orientar recursos no planificados para la atención a dichos grupos, con el riesgo de una eventual confrontación social,

brote de epidemias, surgimiento de actividades ilegales y otros inconvenientes propios de este fenómeno.

Los ciberataques y vulneración de la infraestructura crítica del Estado, que se basan en la explotación de las debilidades de las redes informáticas, ejecutadas a través de mecanismos tecnológicos de ciberterrorismo, ciberdelito, cibercrimen, ciberespionaje, e infiltración de los sistemas informáticos, convirtiéndose en un potente instrumento de agresión contra la infraestructura del Estado, lo cual podría comprometer la seguridad nacional.

Debido al entorno en el que se desarrollan las amenazas y riesgos en el ciberespacio que atentan las redes que gestionan la información y las infraestructuras más sensibles del Estado se hace inevitable mitigar esas amenazas de naturaleza cibernética que son difíciles de identificar y neutralizar debido a la rapidez de su evolución técnica científica, siendo imprescindible la implantación, consolidación y sobrevivencia de una industria de defensa en el país, asociada al fortalecimiento de la matriz productiva, dependiente de nuevas tecnologías, de una constante formación y actualización de recursos humanos altamente calificados en diversas especialidades; conocimientos en los cuales deben estar inmersos los miembros de FF.AA. en el nivel técnico, tecnológico, pre grado y posgrado.

> Dada la importancia estratégica de la seguridad en el ciberespacio, la existencia de ciberamenazas, económicas, asimétricas, anónimas, sin fronteras es imprescindible y prioritario el empleo adicional del personal especializado de FFAA en las denominadas guerras cibernéticas, preparadas para: comandar, explotar y mantener un sistema de Ciberdefensa; alcanzar la capacidad de resiliencia, remediación y respuesta ante ciberataques, incidentes o emergencias informáticas, asumir la misión de defender prioritariamente las instalaciones, redes, servicios y equipos físicos y de tecnología de la información cuya interrupción o destrucción tendría un impacto en el eficaz funcionamiento de las instituciones del sector de la Defensa y del Estado.

Fundamentación. Doctrinaria, Técnica, Documental, Filosófica

Es fundamental que todo el personal militar entienda y tenga totalmente claro lo que establece en la actualidad desde nuestra Constitución de la República en los artículos: 3, 66, 147, 158, 261 y 393; así como también las nuevas misiones asignadas a las Fuerzas Armadas que son “Garantizar la Defensa de la Soberanía e Integridad Territorial” “Participar en la Seguridad Integral” “Apoyar al Desarrollo Nacional en el ejercicio de las Soberanías” y “Contribuir a la paz regional y mundial”; mencionando además que constituye una institución de protección de derechos, libertades y garantías de los ciudadanos. (Asamblea Nacional Constituyente, 2008)

El Plan Nacional de desarrollo Toda una Vida 2017-2021, constituye la normativa que determina nueve objetivos nacionales para el Buen Vivir, así como las políticas y lineamientos estratégicos para construir una sociedad más justa. (SENPLADES, 2012);

El Plan Nacional de Seguridad Integral 2017-2021, establece dos políticas intersectoriales para el sector Defensa, los cuales se relacionan con 5 objetivos nacionales del Buen Vivir (objetivos 2, 3, 6, 7, 9). (Ministerio Coordinador de Seguridad, 2016)

Al conocer todo lo planteado anteriormente el personal militar e inclusive el personal de servidores públicos que laboran en las Fuerzas Armadas estarán en condiciones de dar cumplimiento a las nuevas misiones asignadas, a los nuevos objetivos planteados para la institución y más aún que nuestro personal esté preparado para asumir y enfrentar estos nuevos retos que el gobierno de turno no ha asignado, demostrando de esta manera el profesionalismo que caracteriza a los soldados de honor, cumplidores de las normas y procedimientos que establecen las leyes de la república.

Por otra parte, en la Ley de Seguridad Pública y del Estado expresa en su Art. 11. Los órganos ejecutores del Sistema de Seguridad Pública y del Estado estarán a cargo de las acciones de defensa, orden público, prevención y gestión de riesgos, conforme lo siguiente: a) De la defensa: Ministerios de Defensa, Relaciones Exteriores y Fuerzas Armadas. - La defensa de la soberanía del Estado y la integridad territorial tendrá como entes rectores al Ministerio de

Defensa y al de Relaciones Exteriores en los ámbitos de su responsabilidad y competencia. Corresponde a las Fuerzas Armadas su ejecución para cumplir con su misión fundamental de defensa de la soberanía e integridad territorial. (seguridad, 2014).

La mayoría de las acciones del ciberespacio utilizan el ciberespacio para facilitar otros tipos de actividades, que emplean las capacidades del ciberespacio para completar otras tareas que no son parte de las tres misiones de las Operaciones del Ciberespacio: Operaciones Ofensivas en el Ciberespacio, Operaciones Defensivas en el Ciberespacio y las operaciones del Comando Conjunto.

Esa utilización incluye acciones como la operación de un sistema de C2 o de un sistema logístico, él envió de un email para apoyar un objetivo de información, el uso del internet para completar un curso de entrenamiento online, o para desarrollar un *briefing.* Otros usuarios, que pueden ser usuarios no autorizados de *network*, personal del Comando Conjunto que no necesita una autorización especial para utilizar las capacidades del ciberespacio, etc. En el ciberespacio la mayoría de las vulnerabilidades del sistema del Comando Conjunto, pueden estar expuestas y ser explotadas por nuestros adversarios. El desafío es entrenar a todos los usuarios del Comando Conjunto para comprender el significado de las amenazas del ciberespacio, y a reconocer las tácticas de la amenaza para que el uso del ciberespacio no genere un riesgo innecesario a las operaciones. La protección del ciberespacio del Comando Conjunto mediante el establecimiento de una cultura de prevención de las vulnerabilidades,

particularmente mediante políticas, prácticas y entrenamiento, es crítico para el éxito de todos los tipos de operaciones permitidas en el ciberespacio.

El Ministerio de Defensa Nacional velará por el fortalecimiento de las capacidades operativas pertinentes y desarrollará las políticas específicas en el ámbito aeroespacial, Ciberdefensa, gestión de riesgos, seguridad integral, empleo progresivo de la fuerza contra vuelos ilegales y misiones de inteligencia.[94]

Fundamentación. Histórica, Social, Cultural, etc

Los problemas de límites, los históricos pendientes, la lucha por recursos vitales, las reivindicaciones de tipo religioso, diferencias étnicas, de género, la globalización del comercio entre otros motivos, han generado conflictos entre actores estatales y no estatales, una de las alternativas de solución a sus disputas en los dominios de la tierra, el mar y el aire fue y es aún el uso del poder terrestre, naval y aéreo, conforme los alcanzaban evolutivamente. Es evidente que en el siglo anterior los avances en las técnicas de la información y de las comunicaciones se reflejan en ingenios usados en el cuarto dominio denominado espacial y con mayor impacto en el quinto dominio el ciberespacio, el mismo que además de pulverizar las barreras de tiempo y distancia obligo a establecer nuevos esquemas de defensa a las Fuerzas y Cuerpos de Seguridad para enfrentar los nuevos desafíos del siglo XXI en un teatro de operaciones virtual, el "ciberespacio". En el ciberespacio se desarrollan dos tipos de operaciones: las de Ciberseguridad orientadas a minimizar el nivel de riesgo al que están expuestos

[94] Agenda Política de la Defensa 2018

los ciudadanos ante amenazas de índole cibernético y las de Ciberdefensa encaminadas a garantizar el sentido de seguridad del Estado Nacional.

Las Fuerzas Armadas constituyen el componente militar de la defensa, en el marco de la seguridad, cuyas misiones complementarias no eximen a la sociedad civil y a las demás organizaciones e instituciones públicas y privadas, de compartir el compromiso para alcanzar la soberanía, la defensa de la integridad territorial y de la paz nacional. El poco desarrollo de la cultura de seguridad nacional, dificulta la concientización de que la defensa no es de exclusiva responsabilidad militar sino un concepto y sistema integral en el cual se interrelacionan las esferas política, parlamentaria, judicial, administrativa, económica, educativa y financiera.

Actualmente el Comando Conjunto de las Fuerzas Armadas se encuentra frente a un entorno complejo, incierto y dinámico y es justamente en esa incertidumbre cuando funciona la prospectiva, que es la herramienta utilizada para el diseño del escenario de las Fuerzas Armadas ecuatorianas. Si bien el futuro es imposible de predecir, la prospectiva es una disciplina científica que nos ayuda a reducir la incertidumbre y desentrañar el futuro, si bien es una disciplina relativamente nueva en nuestro medio, en el mundo se viene aplicando desde inicios del siglo XX.[95]

[95] Plan de Gestión Institucional de FF.AA 2010-2021

El escenario o jurisdicción de la Ciberdefensa no solamente abarca el territorio nacional en sus ámbitos terrestre, naval, aéreo, sino que se refiere al CIBERESPACIO que es definido como "La dimensión generada durante el tiempo de interconexión e interoperabilidad de redes, sistemas, equipos y personal relacionados con los sistemas informáticos cualesquiera sean estos y las telecomunicaciones que los vinculan"[96], es así que un incidente o una amenaza en el dominio del ciberespacio puede provenir de cualquier parte del mundo, fuera de la frontera física de un Estado, no solamente desde su interior.

En la actualidad, ya no es posible realizar solo el planeamiento estratégico tradicional, ni en lo político, ni en lo empresarial, ni en lo militar, basados en una “visión” única y siempre deseable para las instituciones; sino que es preciso contar con estrategias claras, además de planes de contingencia basados en diferentes escenarios alternativos, posibles y probables, es aquí donde la prospectiva produce su mayor beneficio.

El Comando Conjunto se ha visto en la obligación de crear diferentes programas que fortalezcan y se ejecuten en base a los objetivos a alcanzar, todo esto realizado sobre los presupuestos asignados, pero siendo claros que la algunos de estos no se pueden cumplir en un tiempo corto, lo que obliga a una planificación por prioridades y apoyadas en el Plan Capacidades Estratégicas Conjuntas.

[96] Apreciación del Comando de Ciberdefensa del CC.FF.AA

En el área de capacidad de Mando y Control se encuentra la capacidad de Protección de la Información (Ciberdefensa), cuyo objetivo es proteger la información contra accesos no autorizados y evitar que esta información sea modificada o manipulada, tanto cuando está almacenada, como cuando se está procesando o en tránsito, y contra la denegación de acceso a usuarios autorizados, incluyendo aquellas medidas necesarias para detectar, documentar y hacer frente a tales amenazas.

Las áreas de capacidades conjuntas del Comando Conjunto de las Fuerzas Armadas se materializan en las siguientes:

g. Mando y Control

h. Vigilancia, Reconocimiento, Inteligencia y Adquisición de Objetivos.

i. Maniobra.

j. Despliegue y Movilidad

k. Supervivencia y Protección.

l. Sostenimiento logístico[97]

Validación de la propuesta.

La presente propuesta se enmarca en bien de los intereses institucionales de Fuerzas Armadas debido a que en la actualidad no solo se enfrenta a un enemigo conocido sino a diferentes amenazas y riesgos que se presentan con el desarrollo de la humanidad. El saber utilizar la información y aprovechar ésta,

[97] Plan de Gestión Institucional del CC. FF. AA 2010 - 2021

obliga a tener un organismo que se encargue de proteger las redes y sistemas informáticos de Fuerzas Armadas y su infraestructura crítica, constituyéndose en parte fundamental para el éxito de las operaciones en cualquier tipo de escenario, es por esto que la guerra de la información se ha convertido en una nueva generación de los conflictos dentro de un país o de una región que entra en esta situación.

La Seguridad en los Estados ha ido cambiando de acuerdo a las situaciones que van desarrollando dentro de él y dentro de su entorno, es así que en los últimos 20 años la informática ha evolucionado mucho, pasando de ser una herramienta administrativa para optimizar procesos de oficina a un instrumento estratégico para la industria, la administración y las Fuerzas Armadas. Antes del 11-S los riesgos y retos de seguridad cibernéticos sólo se trataban dentro de pequeños grupos de expertos, pero a partir de esa fecha resultó evidente que el ciberespacio introduce graves vulnerabilidades en unas sociedades cada vez más interdependientes. Es así como se ve comprometido toda la nación y en general al mundo global, ya que se ha evidenciado que esto es un punto neurálgico y que es vulnerable para la soberanía de los estados, por esta razón este tema es de vital importancia e interés para FF. AA.

Todo lo anterior con lleva a crear una obligación en Fuerzas Armadas, que es proteger la información y la infraestructura crítica. Para que las Fuerzas puedan cumplir su cometido en bien del pueblo ecuatoriano; por ende, se tiene que conocer las diferentes capacidades que un Comando de Ciberdefensa debe poseer para cumplir con su objetivo propuesto. Se tiene que conformar un Comando de Ciberdefensa con capacidades de enfrentar a cualquier tipo de

amenaza que se presente en el ciberespacio. La Fuerzas Armadas requieren tener claramente determinadas las misiones y procedimientos que se deberán cumplir ante los problemas que genera la seguridad de las tecnologías de información en FF. AA; encaminadas a neutralizar las amenazas anteriormente descritas, enmarcadas en políticas claras y con leyes que respalden su accionar.

Conceptualización de la propuesta.

Cuando se habla de Ciberseguridad, se refiere al "conjunto de acciones de carácter preventivo que tienen por objeto el asegurar el uso de las redes propias y negarlo a terceros" y más ampliamente se dice que "conjunto de herramientas, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión de riesgos, prácticas idóneas, y tecnologías que pueden utilizarse para proteger los activos de la organización y de los usuarios en el ciberentorno". Los activos de la organización y los usuarios son los dispositivos informáticos conectados, los usuarios, los servicios, aplicaciones, los sistemas de comunicaciones, las comunicaciones multimedios y la totalidad de la información transmitida y/o almacenada en el ciberentorno.[98]

El ciberespacio en el ámbito mundial, es entendido como el quinto dominio de la guerra, en donde el desarrollo armamentista ya no se enfoca en producir armas, sino utilizando los conocimientos avanzados de las personas conjuntamente con aplicaciones de correlación de información para la toma de decisiones y aplicarla en la ciberguerra, es en ese contexto en el año 2006 el

[98] Información del Comando de Ciberdefensa

Departamento de Defensa de Estados Unidos, explica que el ciberespacio está caracterizado por el uso de la electrónica y del espectro electromagnético para guardar, modificar, intercambiar información a través de los sistemas y redes de la información y las infraestructuras físicas, por tanto actualmente este escenario es considerado como un dominio global dentro del medio de la información compuesto por las interdependientes infraestructuras y redes de la información, incluyendo internet, las redes de telecomunicaciones, sistemas de computadoras, nuevos dispositivos electrónicos y la información en sí.[99]

Cuando se refiere a la seguridad de un estado, se debe entender que estamos hablando de la política de defensa nacional y de esta manera del libro blanco, que es quien da los lineamientos necesarios para el accionar de las Fuerzas Armadas, este momento se está elaborando el libro blanco del año 2018. Por otra parte hay que considerar la perspectiva, es decir tener una visión estratégica, de determinar los principales escenarios, si hay un análisis de los escenarios futuros, se podrán tomar decisiones acertadas, caso contrario, no se podrá planificar, sino se tiene la certeza de estar en las condiciones operativas, lo más probable es que no se tenga éxito en la operación, por consiguiente una visión estratégica de un comandante es muy importante para la toma de decisiones y como dirigirlas, el principal documento que orienta las actividades de las Fuerzas Armadas es la Constitución de la República del Ecuador ya que en su Art 158, nos dice: “Las Fuerzas Armadas tienen como misión fundamental la defensa de la soberanía y la integridad territorial. (Constitución, 2008).

[99] Información del Comando de Ciberdefensa

Se Conoce las capacidades que tiene las Fuerzas Armadas, además conocemos la amenazas y que es lo que quieren realizar estas amenazas y así podemos determinar que podemos realizar, adicional es muy importante la inteligencia, para conocer las intenciones de las amenazas y poder neutralizarla, en la ley orgánica de la defensa Nacional en su Art. 2. Nos dice: “Las Fuerzas Armadas, como parte de la fuerza pública, tienen la siguiente misión: a) Conservar la soberanía nacional; b) Defender la integridad, la unidad e independencia del Estado; y, c) Garantizar el ordenamiento jurídico y democrático del estado social de derecho. Además, nos expresa que debemos colaborar con el desarrollo social y económico del país; se podrán participar en actividades económicas relacionadas exclusivamente con la defensa nacional; e, intervenir en los demás aspectos concernientes a la seguridad nacional, de acuerdo con la ley”. (Orgánica, 2007).

- La Constitución de la República del Ecuador de 2008 en su Artículo Art. 158, nos dice: “Las Fuerzas Armadas sean las encargadas de la seguridad y defensa del territorio nacional.[100].
- Agenda de la Política de la defensa en donde se establecen los campos de acción donde Fuerzas Armadas se emplearán.
- Plan Nacional de Seguridad Integral 2017 – 2021[101].
- Para el cumplimiento de competencias, deberes y responsabilidades en todo el ámbito nacional, el Ecuador utiliza como guía determinante un marco legal establecido, la Constitución de la República, en su Artículo

[100] Constitución Política de la República del Ecuador de 2008.
[101] Plan Nacional de Seguridad Integral 2017 – 2021

158 define como misión fundamental de Fuerzas Armadas la defensa de la soberanía y la integridad territorial.

Método y criterios de Validación.

El método a emplear para la validación de la presente propuesta será la matriz FODA., el cual consiste en orientar principalmente el análisis y resolución de problemas y se lleva acabo para identificar y analizar las Fortalezas y Debilidades de un tema específico, así como las Oportunidades (aprovechadas y no aprovechadas) y todas aquellas Amenazas que pueden poner en riesgo en algún momento la propuesta por la información obtenida del contexto externo y que permitirá a través de su aplicación determinar mecanismos de aplicación.

El análisis FODA, es una herramienta de análisis estratégico que permite, a través de una exploración del ambiente interno y externo de una organización, obtener un diagnóstico preciso de la situación actual de la entidad y del sector al que pertenece y tomar decisiones acordes con los objetivos y políticas formuladas.

Los criterios con los cuales se validará la presente propuesta son:

Fortalezas[102]: Son todas aquellos elementos internos y positivos que poseen nuestras Fuerzas Armadas.

El Estado ecuatoriano concibe intereses nacionales vitales y estratégicos

[102]Nota de Aula Comando de Ciberdefensa COCIBER

para garantizar la soberanía, propender al desarrollo nacional y alcanzar el bienestar de sus habitantes; por consiguiente, tiene la responsabilidad de proteger su territorio, población y recursos frente a cualquier amenaza que atente contra sus intereses.

La defensa nacional constituye un componente esencial de la seguridad nacional que, articulada con la seguridad pública, la política exterior, el apoyo del sistema de inteligencia nacional, garantiza la defensa de la soberanía e integridad territorial y la protección de la población y de los recursos; con los mecanismos de cooperación internacional contribuye a crear un entorno nacional y regional estable y seguro. El Estado al haber definido sus intereses vitales y estratégicos requiere garantizar la vigencia de los mismos; por tanto, al existir amenazas y riesgos que inciden en la consecución de estos, debe estar en condiciones de protegerlos. Es entonces cuando la defensa se constituye en el instrumento para el empleo de la fuerza ante la amenaza externa que atenta contra estos intereses.

La defensa se ejerce con todos los recursos del país, pero las Fuerzas Armadas con sus capacidades, estructura y doctrina son el medio principal para mantener la soberanía e integridad territorial, proteger a la población y los recursos ante amenazas y riesgos cada vez más complejos y difusos. La defensa nacional tiene una relación directa con la política exterior del Estado a fin de garantizar la coherencia de las acciones que se desarrollen en los ámbitos militar y diplomático para el

cumplimiento de sus objetivos. Se orienta por las decisiones soberanas de la política exterior, fundamentadas en los principios del derecho internacional, en la realidad política, económica y social interna y en la situación del entorno internacional. La defensa nacional está orientada a garantizar la paz, la estabilidad y la prosperidad que permitan lograr un desarrollo económico y social sostenible y sustentable, contribuye así a la seguridad integral y al fortalecimiento de la unidad nacional en la diversidad.

Oportunidades[103]: Son los aspectos positivos que podemos aprovechar utilizando nuestras fortalezas, además se debe considerar analizar junto a las amenazas la parte del Análisis Externo, que nos podrían llegar a afectar de manera positiva si somos capaces de capitalizarlas.

Debemos considerar que el ciberespacio ya es un medio o dominio militarmente hablando; que aún no se encuentra completamente definido. Nuevas tecnologías emergentes funcionan sobre el ciberespacio y otras continúan apareciendo tal y como ha sucedido con cloud computing, big data, telefonía móvil e internet de las cosas. A la par nuevas generaciones de usuarios aparecen, las actuales generaciones evolucionan y otras desaparecen: todo ello, con tal de adaptarse a las plataformas instaladas y sus nuevos desarrollos. Estas nuevas generaciones tienen que tener claro que acciones del mundo virtual tienen sus consecuencias en el mundo real. Un claro ejemplo, son los

[103] Nota de Aula Comando de Ciberdefensa COCIBER

problemas causados por los ciberataques, así como las ideas que fluyen en internet, promoviendo percepciones que pueden alterar la paz colectiva y amenazar las soberanías y las estructuras organizacionales. Las redes sociales, hoy por hoy, han probado ser tecnologías emergentes que pueden organizar civiles alrededor de una misma meta, llegando incluso a construir o desorganizar estructuras sociales y políticas de forma impredecible, incontrolable y sin capacidad de anticipación. Con ello, la problemática de seguridad, como consecuencia del uso del ciberespacio, no solo se concentra en temas de técnicos de seguridad en dicho ámbito, sino que implica las consecuencias en el mundo real y sociedad actual, que socaban su continuidad.

En suma, es insoslayable buscar soporte internacional para que esta nueva ola tecnológica no afecte objetivos nacionales, desuna pueblos, o atente aldeas o personas que buscan el mismo fin, o a quienes cambian su sentido de pertenencia y lealtad. El fenómeno está en todos los países del mundo y no solo al nivel del Estado. Sin embargo, para el Ecuador, tras la insuficiente previsión gubernamental en relación al tema, se ha abierto la posibilidad de que se fortalezca la gestión tecnológica de infraestructura e información nacional desde el exterior hacia el país. De ahí que es imprescindible rediseñar la organización de la política de la Ciberdefensa en todos sus niveles y la implementación de una Secretaría de Ciberdefensa que permitirá una política de la privacidad y la gestión de la información en la sociedad ecuatoriana y con ello el mejoramiento de la seguridad en la infraestructuras críticas vitales para la propia

existencia del Estado y la sociedad ecuatoriana en su conjunto, siendo así se estaría implementando una doctrina de Ciberdefensa con el propósito de aprovechar el apoyo del nivel político – estratégico y estratégico – militar que posee el Comando de Ciberdefensa.

Debilidades[104]: Entendidas como problemas internos, que una vez identificados y desarrollando una adecuada estrategia, pueden y deben eliminarse.

La no existencia de doctrina de Ciberdefensa a nivel, recae en una falta de cultura de seguridad informática en todos los niveles, constituyéndose en el principal problema. Por tal razón existe un gran vacío doctrinario, en vista de que no existe personal capacitado, planes y Procedimientos establecidos, una doctrina que sustente el desarrollo de las actividades de Ciberdefensa en el país, contra el incremento de nuevas formas de ataques informáticos, amenazas y ciberdelitos.

Como estrategia se considera establecer una doctrina base que sirva de lineamiento para la ejecución de las operaciones de Ciberdefensa, capacitar al personal del Comando, esta capacitación debe ser orientada tanto en la parte técnica como en los procesos de gestión para el manejo de incidentes, para lograr este objetivo finalmente es la de realizar una campaña en coordinación con G-6 para que se den charlas y conferencias de seguridad informática a todo el personal de FFAA.

[104] Nota de Aula Comando de Ciberdefensa COCIBER

Propensa a crear en el personal militar una cultura de seguridad informática.

Amenazas[105]: Son todas aquellas actividades o situaciones que implican o conllevan riesgos de daños, trastornos y efectos nocivos para la seguridad en uno o más campos de la actividad nacional. Son provocadas, ejecutadas o causadas por opositores, adversarios o enemigos del Estado, internos o externos. Las amenazas, al materializarse, se convierten en conflictos que atentan contra la Seguridad y Defensa Nacional.

Las amenazas globales tienen una connotación transnacional que podría afectar a la defensa y seguridad de los Estados. Entre otras, podemos señalar: el terrorismo, narcotráfico y sus delitos conexos, crimen organizado, ciberataques, exploración y explotación ilegal de los recursos marítimos, delincuencia organizada transnacional.

[105] Nota de Aula Comando de Ciberdefensa COCIBER

Validación.

Matriz de Cuadrícula.

FORTALEZAS	DEBILIDADES
1. Personal técnico experimentado, con título de tercer y cuarto nivel en temas de TIC's y afines. 2. Disponer de una estructura orgánica aprobada que viabilizo la creación del COCIBER. 3. Disponer de presupuesto para la ejecución del Proyecto de Implementación de las Capacidades de Ciberdefensa. 4. Las FF.AA. a lo largo de su historia, se ha caracterizado por ser una institución cimentada en valores y principios como la disciplina, honor y lealtad y su entrega irrestricta a la defensa de la Patria	1. Falta de aspectos doctrinarios que deber ser tomados en consideración para el desarrollo de las capacidades del ciberespacio. 2. Falta de procesos y procedimientos para el cumplimiento de la misión del Comando. 3. Carencia de infraestructura física y tecnológica 4. Falta de capacitación especializada en temas de Ciberdefensa y Ciberseguridad. 5. Personal insuficiente para cubrir el área operativa. 6. Falta del presupuesto para el cumplimiento de la gestión administrativa y logística del Comando.

OPORTUNIDADES	AMENAZAS
1. Apoyo del nivel político - estratégico y estratégico – militar. 2. Esfuerzos políticos nacionales y regionales para temas de colaboración en Ciberdefensa y Ciberseguridad. 3. Oferta académica nacional e internacional relacionadas a temas de TIC´s, seguridad informática y Ciberdefensa. 4. Acceso a las TIC´s y amplia oferta de proveedores, herramientas especializadas, hardware y software.	1. Falta de un Marco Legal que respalde nuestro accionar. 2. Desarrollo de nuevas formas de ataques informáticos e incremento de amenazas y ciberdelitos. 3. La falta de cultura de la seguridad la informática en todos los niveles. 4. Falta de gestión de seguridad informática en FF.AA. 5. No se encuentra definida la Infraestructura Crítica digital de FF.AA. 6. Carencia de cooperación interinstitucional nacional e internacional en el ámbito de Ciberdefensa. 7. El incremento del uso a las nuevas tecnologías genera mayor vulnerabilidad a la seguridad.

Capítulo VI

CONCLUSIONES Y RECOMENDACIONES

Conclusiones

Desde el punto de vista de la Ciberdefensa el análisis prospectivo del CC.FF.AA hace referencia a la constante amenaza ciberespacial, con la posibilidad de colapsar e incluso dañar físicamente los sistemas de información. Y de acuerdo al P.N.S.I 2014-217 hace referencia a la Ciberdefensa en la estrategia 1.3 Desarrollar las capacidades de Ciberdefensa, y en la 1.4 Desarrollar acciones de Ciberdefensa que permitan defender la infraestructura critica, las redes y la información electrónica en el ámbito de la Defensa.

Se crea el Comando de Ciberdefensa del CC.FF.AA integrado por personal técnico y operativo, militar y servidores públicos, con la misión de operar las capacidades de Defensa, Exploración y Respuesta en el espacio cibernético, para proteger y defender la infraestructura crítica e información estratégica del Estado.

Actualmente el Comando de Ciberdefensa se encuentra como una capacidad del área de mando y control, la misma que tiene tres sub capacidades o capacidades específicas: prevención, detección y respuesta. Además, no se encuentra el detalle de las actividades que cumple cada una de ellas.

Las amenazas de la Ciberdefensa se encuentran acorde a las nuevas amenazas cibernéticas que consideran la mayoría de los países del mundo, razón por el cual se debe tomar las medidas necesarias para afrontar de la mejor manera a las siguientes Ciberamenazas:

- Ciberamenazas:
  - ✓ Ataques contra infraestructura crítica.
  - ✓ Ataque contra las redes y sistema.
  - ✓ Ataque contra los servicios de internet.
  - ✓ Ataque contra los sistemas de control y redes industriales.
  - ✓ Infección con malware.
  - ✓ Ataque contra redes, sistemas o servicios a través de terceros.
- Ciberdelincuentes
- Ciberespionaje
- Ciberterroristas
- Hacking

La operabilidad y operatividad del Comando de Ciberdefensa actualmente se encuentra aproximadamente al 5% de su capacidad operativa, cabe mencionar que aquí también se incluyen las tres Fuerzas, es decir, un nivel muy bajo, por lo que las actividades del COCIBER se encuentran muy limitadas.

El COCIBER no dispone de una matriz que permita determinar la capacidad operativa como tienen los demás sistemas operativos del campo de batalla.

Propuesta

a. Que la Ciberdefensa sea considerada directamente un área de Capacidad del Comando Conjunto de las FF. AA y no como una capacidad del Mando y Control como se encuentra actualmente, de acuerdo al siguiente detalle:

1) Grupo de DEFENSA, mediante operaciones de Ciberdefensa orientadas a:
   a) La protección de los sistemas de información y comunicaciones, a través de la anticipación, prevención, monitorización, análisis, detección, predicción, resistencia, mitigación frente a intrusiones, perturbaciones, interrupciones o cualquier acción que comprometa la información y los sistemas propios.
   b) Determinar vulnerabilidades de sistemas propios e identificar posibles Ciberamenazas o Ciberincidentes.
2) Grupo de EXPLORACIÓN, mediante operaciones de Ciberexploración orientadas a obtener información, determinar y actualizar las capacidades de Ciberdefensa del enemigo o de potenciales adversarios y agentes hostiles, a través de actividades de recopilación, análisis, valoración y exploración de información.
3) Grupo de RESPUESTA, mediante operaciones de Ciberespuesta orientadas a:

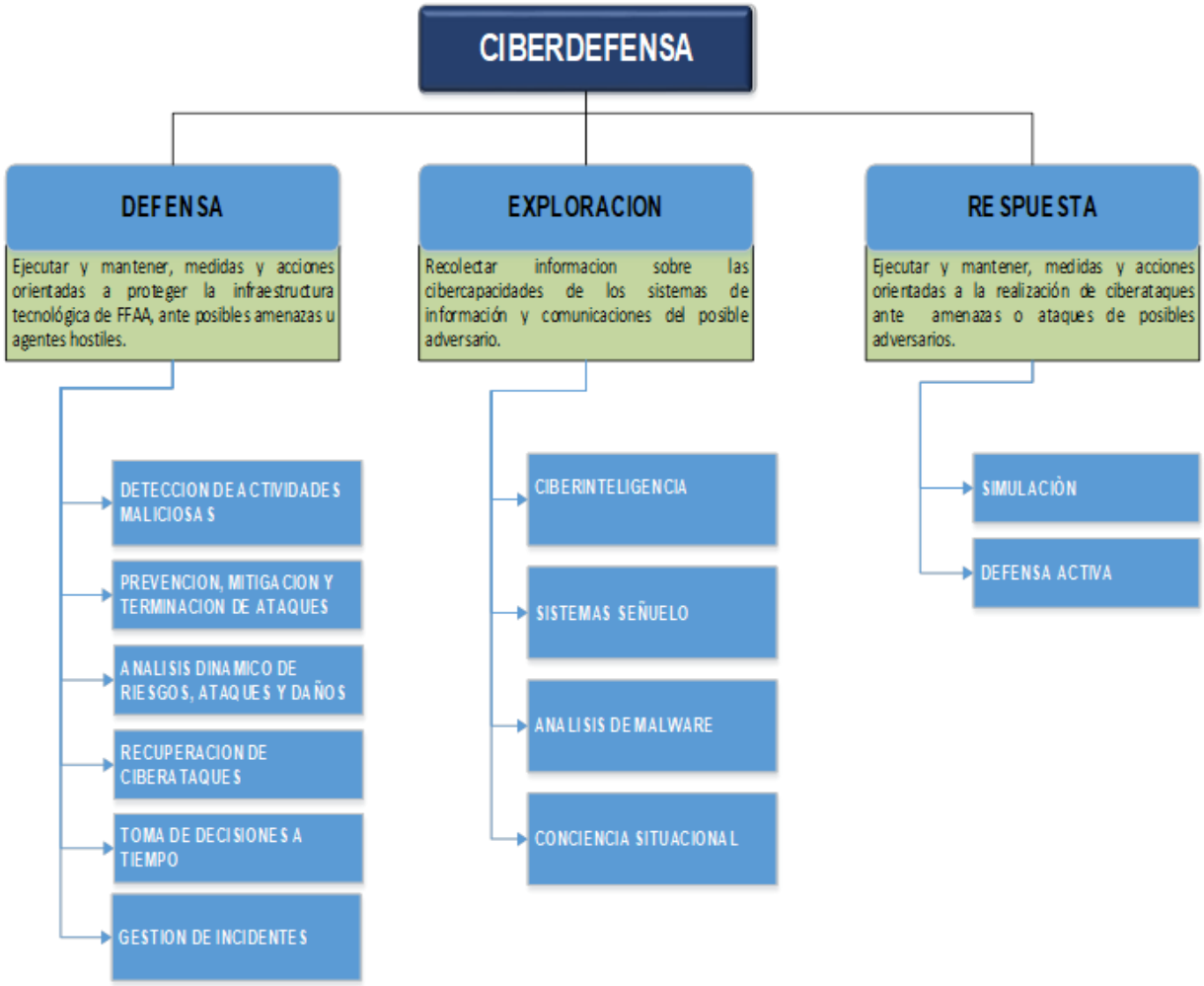
   Mediante acciones ofensivas o ciberataques (DDOS, ATAQUES), para minimizar o bloquear los sistemas de información e

infraestructura crítica del enemigo, o frente a amenazas o ataques de adversarios y agentes hostiles, a través de:

- Operaciones de Inteligencia digital.
- Operaciones contra la integridad de datos
- Operaciones de denegación de servicios
- Operaciones de infección
- Operaciones de infiltración

Figura N° 10.

Propuesta de Sub-capacidades o capacidades específicas del COCIBER



b. El proyecto para Aumentar la capacidad operativa del Comando de Ciberdefensa en formato SENPLADES 2015-2017[106] se requiere que se ejecute lo más pronto posible, con el fin de implementar toda la infraestructura necesaria, capacitación especializada al personal militar y proteger la infraestructura crítica digital de Fuerzas Armadas, con esto se logra alcanzar un 75% de la capacidad operativa.

c. Para establecer la capacidad operativa del COCIBER se propone inicialmente hacer una matriz en la que conste los siguientes componentes en base a la misión que cumple en la defensa del territorio nacional, ámbito interno y gestión de riesgos:

Tabla 3

Propuesta de matriz general inicial de capacidad operativa del COCIBER

MATRIZ DE CAPACIDAD OPERATIVA DEL COCIBER DEL CC.FF.AA			
	FUERZA	**COMPONENTE**	**PORCENTAJE (%)**
MISIÓN	COCIBER FUERZA TERRESTRE FUERZA NAVAL FUERZA AÉREA	• PERSONAL, CAPACITACIÓN Y ENTRENAMIENTO.	30
		• MATERIAL Y EQUIPO.	20
		• EQUIPAMIENTO DE SOFTWARE Y LICENCIAMIENTO.	25
		• INFRAESTRUCTURA TECNOLÓGICA.	25
	TOTAL		100

[106] proyecto para Aumentar la capacidad operativa del Comando de Ciberdefensa en formato SENPLADES 2015-2017, el cual se encuentra presentado pero hasta el momento no se ha ejecutado.

Recomendaciones

Mejorar los procedimientos a seguir, que permita disponer de la información suficiente en tiempo real del personal empleado y las actividades que estas están ejecutando, por parte del Ministerio de Defensa y Comando Conjunto para que no interfiera sus disposiciones en el desarrollo de las actividades planificadas y que se estén ejecutando.

Para ejecutar un apoyo eficiente y eficaz a los organismos del Estado, frente a las múltiples amenazas se debe capacitar y entrenar al personal militar en este tipo de escenarios, debiéndose impartir los conocimientos respectivos en las escuelas de formación, perfeccionamiento y especialización y sean estos conocimientos parte de los contenidos en las mallas curriculares, para lo cual si es el caso se debe actualizar, adaptar, modificar o ampliar la doctrina establecida para este tipo de escenarios en los cuales está inmerso estas nuevas amenazas y proteger la infraestructura crítica del Estado.

El Ecuador constituido como estado soberano, tiene la obligación de proteger su Infraestructura Estratégica, en especial aquella considerada como CRÍTICA, pues su interrupción o neutralización causaría grave impacto y repercusiones de carácter estratégico en su normal desarrollo y funcionamiento, generando desequilibrio económico, político y social.

En el Ecuador el uso del internet se ha cuadruplicado desde el año 2006, incrementando el acceso a la información, de todos los estratos sociales. La conectividad hasta el 2019 se sustentaba en más de 8.000 Km., de fibra óptica,

sin embargo, aún persiste una gran brecha entre lo rural y lo urbano; pero ahora se sustenta en un cable de fibra óptica submarino de 40.000,00 Km. de longitud enterrado en el lecho marino que se extiende desde las costas de Florida-EEUU directamente hasta Manta-Ecuador, permitiendo conectividad a más de 60.000,00 Km. de redes internas de banda ancha del país. Pese a que el Ecuador se encuentra bajo la media latinoamericana en gobierno electrónico, existe voluntad política para que la mayoría de la ciudadanía tenga a futuro la mayoría de servicios públicos en red.

Para garantizar la defensa de la soberanía e integridad territorial y participar en la seguridad integral, la Agenda Política de la Defensa 2018, prevé realizar operaciones de protección del espacio cibernético y operaciones de protección a las áreas de infraestructura estratégica (crítica digital). Por lo tanto, para el empleo de Fuerzas Armadas en la protección de la información estratégica y la infraestructura crítica del país, así como de las redes y la información electrónica, se requiere dotarle de medios y recurso necesarios a través del desarrollo e implementación de la Capacidad Estratégica Conjunta de Ciberdefensa.

Es conocido que la capacidad actual de Fuerzas Armadas y del Estado para enfrentar las amenazas en el espacio cibernético, actualmente es limitada, constituyendo una vulnerabilidad que puede ser aprovechada por terceros para realizar sabotajes en la Infraestructura Crítica Digital; denegar servicios básicos a la ciudadanía, adulteración de identidad para apropiarse de cuentas electrónicas de autoridades de la Defensa (phishing), entre otros.

Kaspersky Lab; anunció en agosto del 2014[107], el descubrimiento de una activa campaña de espionaje cibernético en América Latina, denominada "Machete", la misma que ha contado entre sus víctimas a gobiernos especialmente sudamericanos, militares de alto rango, embajadas y agencias estatales; la mayoría de los cerca de 870 objetivos de "Machete" estarían en Venezuela (52%), Ecuador (38%), Colombia (17%), Perú y Cuba – pero hay otros países afectados, entre ellos Rusia y España. Así mismo una proyección al 2019 de datos estadísticos de inteligencia recopilados con la tecnología KSN (*Kaspersky Security Network*)[108], entre varios análisis, ubican al Ecuador en el 5to lugar con 7'629.962 intrusiones cibernéticas, de un universo de 17 países latinoamericanos; esto dentro de la distribución geográfica de los incidentes de los ataques registrados fuera de línea (off-line), en donde los criminales utilizan otros medios de infección cómo los dispositivos USB.

El Ministerio de Defensa Nacional consciente de la magnitud de la amenaza para Fuerzas Armadas y el Estado, con Acuerdo Ministerial Nro. 281 del 12 de septiembre del 2014, dispone la creación del Sistema de Ciberdefensa como mecanismo que articule las instancias permanentes y de conformación para abordar el tema desde el nivel político - estratégico, estratégico - militar y operacional; a fin de coordinar e implementar políticas y estrategias de Ciberdefensa, así mismo se dispone la conformación del Comando de Ciberdefensa como un Comando Operacional del Comando Conjunto de las FF.AA., integrado por personal técnico y operativo civil y militar.

[107] http://www.viruslist.com/sp/weblog?weblogid=208188998
[108] http://latam.kaspersky.com/analisis2014pronosticos2015LatAm

La Agencia de Regulación y Control de las Telecomunicaciones, informo acerca del incremento de los ataques a los servicios en línea, la progresiva sofisticación en las aplicaciones para el ataque y espionaje a las TIC´s del Gobierno e Infraestructuras Críticas del Estado.

Hay que considerar que el grado de conocimiento que necesita un atacante para agredir a los sistemas de información y comunicaciones, ha decrecido a lo largo del tiempo debido al espectacular aumento de la calidad, cantidad y disponibilidad de herramientas ofensivas. Actualmente, es relativamente fácil encontrar en Internet una variedad de herramientas para penetrar o vulnerar redes. La protección de las infraestructuras críticas se presenta como un reto para las Instituciones públicas y privadas, aunque en ocasiones se desconoce las consecuencias potenciales de estos ataques; por lo que es imprescindible tomar acciones en el campo de la Ciberdefensa de manera integral, evitar iniciativas aisladas con visiones diferentes, considerando que la sofisticación de los ataques cibernéticos hace imposible la protección tradicional con mecanismos aislados.

Enfrentar las amenazas cibernéticas, no solamente es responsabilidad de FFAA, para enfrentarlas se requiere el trabajo sistematizado de varias entidades del Estado orientados a la normalización, estandarización, emisión de políticas públicas, organización, cooperación nacional e internacional; con un adecuado desarrollo de cultura de seguridad. Bajo esta premisa y de acuerdo con las

normas ISO 27001[109], la Ciberdefensa debe ser tratada y enfocada a los tres pilares fundamentales de la Seguridad de la Información (integridad, disponibilidad y confidencialidad) realizando una planeación estratégica que debe estar enfocada hacia dónde están evolucionando las amenazas y riesgos de seguridad en el ámbito global.

Ante las amenazas y riesgos en el ciberespacio orientadas a la infraestructura crítica digital, sin la capacidad de enfrentarlas adecuadamente, se puede identificar al problema como la indefensión en la que se encuentra Fuerzas Armadas; sin la posibilidad de cumplir su misión fundamental de garantizar la soberanía y defensa del territorio nacional.

Fortalecer la capacidad de FF.AA. para enfrentar las amenazas que atentan contra su seguridad y defensa en el ámbito cibernético (Ciberdefensa y Ciberseguridad), creando el ambiente y las condiciones necesarias para minimizar sus efectos en su infraestructura Tecnológica, Información y Comunicaciones, en apoyo a la planificación de las operaciones y en el asesoramiento al mando para la toma de decisiones adecuadas.

Implementar la capacidad estratégica conjunta de Ciberdefensa y fortalecer las capacidades específicas de cada una de las Fuerzas para minimizar o neutralizar las amenazas y factores de riesgo que atenten contra la infraestructura crítica digital de la defensa.

[109] http://www.normalizacion.gob.ec/wp-content/uploads/downloads/2019/EXTRACTO_2019/GAN/nte_inen_iso_iec_27000extracto.pdf

El problema fundamental para la Defensa es el cambio que las nuevas tecnologías han producido. Si en el pasado era suficiente con aprovecharse de las nuevas capacidades de los sistemas de información y del ciberespacio para mejorar la eficacia operacional de las Fuerzas Armadas, ahora es necesario poder combatir y ganar, en el ciberespacio.

La Defensa requiere asegurar las capacidades en el ciberespacio para poder garantizar la efectividad en las operaciones tradicionales. Se ha dicho del ciberespacio que es el campo de batalla del futuro.

Este cambio obliga a modificar los conceptos y doctrinas que se aplican a la confrontación clásica, que deben ser adaptados a las exigencias de un escenario virtual asimétrico. Este proceso adaptativo debe ser el punto de partida para la definición sólida y la creación ordenada de una Capacidad Estratégica de Ciberdefensa

BIBLIOGRAFÍA

Ardieta, L. (2013). Capacidades Esenciales para una Ciberdefensa. Cybersecurity Research Group.

Astigarraga, E. (2016). Grandes tendencias políticas y sociales de interes para la seguridad y la defensa . Deusto Business School, de la Universidad Deusto en San Sebastián.

Asamblea Nacional Constituyente. (2008). En A. N. Constituyente. Quito.

Badillo. (2011). Guerra Cibernetica la nueva amenaza.

Clarke, K. &. (2017). Guerra en la Red.

Constitución. (2008). Constitución de la República del Ecuador. Montecristi: Ecuador.

Cornaglia, S. (2017). La Ciberdefensa y su regulacion legal en Argentina. Revista Latinoamericana de Estudios de Seguridad, 46-62.

Castellanos. (2018). http://www.bioestadistico.com/index.php?option=com_content&view=article&id=153:calculo-del-tamano-de-la-muestra-para-estimar-parametros-categoricos-en-poblaciones-finitas&catid=46:calculo-del-tamano-de-la-muestra&Itemid=213. Obtenido de http://www.berrie.dds.nl/calcss.htm

Defensa, M. d. (2018). Amenazas y Riesgos a la Defensa y Seguridad Del Estado. Quito: Ministerio De Defensa.

Defensa, M. d. (2018). Politicas de la Defensa Nacional "Libro Blanco". Quito: Ministerio de Defensa y CC.FF.AA.

Defensa, P. d. (2018). *Agenda Política de la Defensa.* Quito: Ministerio de Defensa .

DEPARMENT OF THE ARMY UNITED STATES OF AMERICA. (2015-2018). Cyberspace Operations. The Department of Defense Cyber Strategy.

Astigarraga, E. (2008). *Análisis Prospectivo Escenario.* Deusto Business School, de la Universidad Deusto en San Sebastián.

Fabregat. (2013). La geopolìtica Cibernètica . revista de geopolìtica, 14-35.

Clarke, K. &. (s.f.). Guerra en la Red. 2011.

Freire, B. (2016). Aplicación de la Ciberdefensa en la Seguridad Nacional. Revista Presencia la Asociación de Generales, 59-65.

Fuertes, W. (2017). Ciberseguridad y Ciberdefensa. CESPED.

GANUZA, N. (2015). CIBERSEGURIDAD. RETOS Y AMENAZAS. En M. D. DEFENSA, CIBERSEGURIDAD. RETOS Y AMENAZAS A LA SEGURIDAD NACIONAL EN EL CIBERESPACIO. MADRID ESPAÑA: NIPO: 075-11-013-6 (edición en línea).

Knabe, C. &. (s.f.). La Ciberguerra. 2011.

Licha. (2000). *La contrucción de escenarios.* Washington D.C.

Ministerio Coordinador de Seguridad. (2016). Plan Nacional de Seguridad Integral.

Nacional, M. d. (Diciembre 2018). Políticas de La Defensa Nacional Del Ecuador "Libro Blanco". Quito - Ecuador: Instituto Geográfico Militar.

Orgánica, L. (2007). Ley Orgánica de la defensa Nacional. Quito: Ecuador.

OTAN. (s.f.). Obtenido de http://www.nato.int/docu/review/2011/11-september/Cyber-hreads/ES/index.htm

Pérez, G. &. (2018). Infraestructura y Tècnicas de alistamiento de reclutas para Ciberguerra. Madrid.

Pérez, G. &. (2015). *Infraestructura y Tècnicas de alistamiento de reclutas para Ciberguerra.* Madrid.

seguridad, L. (2014). Ley de Seguridad Pública y del Estado. Quito: Ecuador.

SENPLADES. (2016). El Plan Nacional de desarrollo Toda una Vida.

Soriano. (2017). Los dilemas estratégicos de la ciberguerra. Ejército de Tierra Española, 14-19.

Zea, F. (2013). Ciberdefensa Militar. Revista Española de Defensa, 48 - 54.

ANEXOS