Facultad del Ejército
Escuela Superior de Guerra
"Tte Grl Luis María Campos"

TRABAJO FINAL INTEGRADOR

Título: "Ciberdefensa y ciberseguridad en las operaciones militares en el Comando de Operaciones de Defensa Interna de Paraguay"

Que para acceder al título de Especialista en Conducción Superior de OOMMTT presenta el Mayor Celso Ariel Martínez Machuca.

Director de TFI: CR (R) Mg OMAR LOCATELLI

Cuidad Autonoma de Buenos Aires, 5 de julio de 2023

Resumen

La presente investigación, realiza el analisis y desempeño operativo sobre “Ciberdefensa y ciberseguridad en las operaciones militares del Comando de Operaciones de Defensa Interna (CODI) de Paraguay’’.

Es un estudio bibliográfico de autores en materia de operaciones de defensa interna, como de especialistas en ciberdefensa y que corresponde a un diseño explicativo con técnicas de validación fijadas en el análisis bibliográfico, lógico y entrevista.

Se inicia con una descripción de la situación y se identifican las ciberamenzas que podrian afectar las operaciones militares en los departamentos afectados con el decreto presidencial de empleo de elementos de combate de las Fuerzas Armadas de la Nacion, que son; Concepción, San Pedro y Amambay.

Posteriormente, se describe el empleo de ciberdefensa y ciberseguridad en las operaciones militares relacionadas a las señales electromagnéticas desarrolladas por las fuerzas y se determina el empleo mas adecuados para ser implementados contra grupos criminales organizados o elementos de las fuerzas de insurgencia que operan en los departamentos mencionados en el decreto presidencial.

Finalmente, se identifica personal y equipos especiales necesario para el empleo de ciberdefensa y ciberseguridad, para proteger las operaciones militares en la utilización de informaciones sensible a la seguridad nacional.

Palabras Claves: Ciberdefensa y ciberseguridad – Operaciones militares – Comando de Operaciones de Defensa Interna.

ÍNDICE

Introducción

Antecedentes y justificación del problema

Paraguay, comenzó el abordaje de esta temática desde un contexto de necesidad y una perspectiva orientada hacia lo concerniente a la seguridad informática; aun así, la ciberdefensa no ha sido tratada para integrar las capacidades del instrumento militar dentro del sistema de ciberdefensa como un comando, en respuesta a las pautas establecidas por el estado paraguayo.

Si bien, se continúa con el desarrollo a través de la creación de los organismos que formarían parte de ella y de su adecuación a lo establecido en la legislación vigente de la defensa, es útil remarcar que, en la actualidad, este documento continúa en proceso de actualización y que el instrumento militar carece de una doctrina de ciberdefensa que defina su empleo dentro del ciberespacio.

Desde el año 2013, las Fuerzas Armadas (FF.AA.) de la República del Paraguay, a traves de la creacion del Comando de Operaciones de Defensa Interna (CODI), con otras instituciones de seguridad como la Policía Nacional (PN), la Secretaría Nacional Antidrogas (SENAD) y el Ministerio Público (MP) a través de la fiscalía, están siendo empleadas en las operaciones de defensa interna en algunos departamentos al norte del país en contra de las acciones de grupos armados al margen de la ley, que afectan las condiciones de desarrollo y seguridad nacional de acuerdo a la modificacion de la ley Nº 5036 / que modifica y amplía los artículos 2º, 3º y 56 de la ley Nº 1.337/99 “De Defensa Nacional y de Seguridad Interna” que meciona lo siguiente:

Artículo 1º.- Modíficanse y amplíanse los artículos 2º, 3º y 56 de la Ley Nº 1.337/99 “DE DEFENSA NACIONAL Y SEGURIDAD INTERNA”, que quedan redactados de la siguiente forma:

“Art. 2º.- La defensa nacional es el sistema de políticas, procedimientos y acciones desarrollado exclusivamente por el Estado para enfrentar cualquier forma de agresión externa

e interna que ponga en peligro la soberanía, la independencia y la integridad territorial de la República, o el ordenamiento constitucional democrático vigente."

"Art. 3º.- A los efectos de la presente ley, se entenderá:

a) Por soberanía: el poder supremo del Estado por sobre cualquier otra institución u organización de cualquier naturaleza, sin más límite que lo establecido en la Constitución Nacional y en las leyes.

b) Por independencia: la existencia de la República del Paraguay en la comunidad internacional como un Estado regido única y libremente por su Constitución Nacional, los tratados internacionales vigentes, de acuerdo con lo establecido en el artículo 141 de la Constitución Nacional, sus leyes y sus autoridades.

c) Por integridad territorial: la inviolabilidad e inajenabilidad del territorio, de las aguas territoriales y del espacio aéreo de la República del Paraguay.

d) Por autoridades legítimamente constituidas: por aquellas electas o designadas, de acuerdo con el ordenamiento constitucional y democrático vigente.

e) Por defensa de las autoridades legalmente constituidas: el conjunto de medidas y acciones que garanticen el libre ejercicio de sus funciones constitucionales y legales."

"Art. 56.- Sin perjuicio de lo estatuido en el artículo 51, durante la vigencia del Estado de Excepción, o frente a situaciones de extrema gravedad en que el sistema de seguridad interna prescripto en esta ley resulte manifiestamente insuficiente, el Presidente de la República podrá decidir el empleo transitorio de elementos de combate de las Fuerzas Armadas de la Nación, exclusivamente dentro del ámbito territorial definido por Decreto y por el tiempo estrictamente necesario para que la Policía Nacional o, en su caso, la Prefectura General Naval, estén en condiciones de hacerse nuevamente cargo por sí solas de la situación.

En esa circunstancia, el Presidente de la República tendrá la conducción de todas las fuerzas militares y policiales afectadas, y podrá designar un comandante de las operaciones de

esas fuerzas, en cuyo caso estas le quedarán subordinadas exclusivamente en el ámbito territorial y por el tiempo definido en el Decreto respectivo.

Tratándose de una forma excepcional, temporal y localizada, de empleo de elementos de combate, ella no incidirá en la doctrina, disciplina, cadena de mandos, organización, equipamiento y capacitación de las Fuerzas Armadas de la Nación, ni autorizará acciones fuera de la ley o que de alguna manera entorpezcan el regular funcionamiento de los Poderes del Estado.

Igualmente se aplicará este procedimiento en los casos calificados como terrorismo de conformidad a la Ley Nº 4.024/10 "QUE CASTIGA LOS HECHOS PUNIBLES DE TERRORISMO, ASOCIACIÓN TERRORISTA Y FINANCIAMIENTO DEL TERRORISMO", o cuando existieren amenazas o acciones violentas contra las autoridades legítimamente constituidas que impidan el libre ejercicio de sus funciones constitucionales y legales.

Dentro de las cuarenta y ocho horas, el Presidente de la República dará cuenta al Congreso de la Nación de su decisión de emplear transitoriamente elementos de combate de las Fuerzas Armadas de la Nación, con adjunción de copia autenticada del Decreto respectivo, pudiendo el Congreso decidir la cesación de esa intervención operativa de las Fuerzas Armadas."

Con esta modificacion de la Ley de Defensa Nacional el Presidente de la Republica del Paraguay en su carácter de Comandante en Jefe de las Fuerzas Armadas de la Nacion emite el Decreto Presidencial 101/13, que menciona lo siguiente:

"Art. 1°.- Dispónese el empleo de elementos de combate de las Fuerzas Armadas de la Nación en Operaciones de Defensa Interna, en los Departamentos de Concepción, San Pedro y Amambay, con la finalidad de garantizar la seguridad interna, dentro del marco legal

establecido en la Ley N° 5036/13 que modifica la Ley Nº 1337/99 "De Defensa Nacional y Seguridad Interna".

Estos grupos armados al margen de la ley que operan generalmente en los departamentos de Concepción, San Pedro y Amambay, donde ejercen gran influencia sobre la población por la situación de necesidades existentes, la frontera seca con el Brasil y la escasa presencia de las instituciones del estado.

Se observan hechos delictivos constante en los departamentos mencionados que van desde asaltos a transportadores de caudales, crimen organizados, extorsion, arma trafico, narcotraficos, el grupo insurgente autodenominado guerrilla que realiza cobro de impuestos revolucionarios, secuestros y asesinatos.

Todas estas acciones realizadas, tiene como objetivo delicuencial ejercer control total o parcial sobre una parte del territorio paraguayo, poseen gran capacidad economica para compras de distintos paratos tecnologicos de uso civil, comercial o inclusive militar para captar informacion que sean emitidas a traves de las señales electromagneticas por los organismos de la seguridad nacional a cargo del Comando de Operaciones de Defensa Interna (CODI) y que pueda ser de utilidad en sus acciones a estos grupos armados al margen de la ley. Por tal motivo, se considera importante el empleo de ciberdefensa y ciberseguridad en las operaciones militares a las acciones realizadas por el Comando de Operaciones de Defensa Interna (CODI).

Actualmente, Paraguay cuenta con un Plan Nacional de Ciberseguridad, es un documento estratégico que sirve como fundamento para la coordinación de las políticas públicas de ciberseguridad, integrando a todos los sectores en el desarrollo de las tecnologías de la información y comunicación (TIC) en un ambiente cibernético confiable y resiliente. (MITIC, 2017)

Este plan, que se encuentra aprobado mediante decreto del poder ejecutivo 7052/17, a través del Ministerio de Tecnologías de la Información y Comunicaciones (MITIC) y en

coordinación con el Ministerio de Relaciones Exteriores (MRE), con la participación de los diversos sectores involucrados en ciberseguridad en Paraguay, bajo el apoyo y facilitación de la Organización de los Estados Americanos (OEA). (MITIC, 2017)

Las Fuerzas Armadas, a traves del Ministerio de Defensa Nacional cuenta con una política de ciberdefensa aprobada por resolución Nº 573 de fecha 04 de octubre de 2021, que permitió establecer los objetivos y lineamientos específicos para la protección del ciberespacio. (Ciberdefensa, 2021)

A partir de allí, se redactan las doctrinas correspondientes al área que incluye al campo militar, desencadenando varios planes concerniente a ciberseguridad y ciberdefensa dentro del cual lógicamente se incluyó lo que corresponde a la misión constitucional de las Fuerzas Armadas de la Nación, como responsable de la soberanía y seguridad nacional.

En la actualidad, no se entiende a los conflictos modernos solo en los espacios tradicionales como tierra, agua y aire, sino que se han agregado nuevos ambientes operacionales como el ciberespacio.

La llegada y evolución del espacio cibernético ha transformado el mundo y revolucionado la vida diaria de los habitantes del globo. Al igual que en el mar, la tierra o el aire, el espacio cibernético es un dominio en el que los seres humanos maniobran en y a través de él para lograr objetivos en los espacios físicos donde viven. No tiene fronteras geográficas, la tecnología es barata y se encuentra al alcance de cualquiera, la autoría de acciones perniciosas es anónima, y sus autores oscilan desde adolescentes hasta organizaciones criminales, algunas independientes y otras, que aparecen como tales, son apoyadas por algunos gobiernos. (Vergara, 2016)

El Comando de las Fuerzas Militares de Paraguay, se encuentra en los pasos iniciales para establecer la forma adecuada de abordar el empleo de ciberdefensa y ciberseguridad en las operaciones militares.

La politica de ciberdefensa, tiene como finalidad orientar las acciones del Ministerio de Defensa Nacional, en el nivel estrategico, operacional y tactico, para lograr los objetivos trazados en el ciberespacio para su aplicación en el ambito de la expresion militar proyectado al poder y potencial nacional. (Ciberdefensa, 2021)

Los objetivos de la politica de ciberdefensa se redactan en base a la intencion establecida dentro de la politica de defensa nacional de la República del Paraguay que en su presentacion menciona “Esta Politica Nacional de Defensa (PND), fue elaborada ante la necesidad de prevenir y combatir eficientemente las nuevas amenazas; tales como el terrorismo, los secuestros, el crimen organizado transnacional, el narcotrafico, los grupos armados ilegales, los ataques ciberneticos, entre otras; sin descuidar las amenazas tradicionales para la República del Paraguay” (Ciberdefensa, 2021)

Citando, como objetivos la de garantizar el uso efectivo del ciberespacio a traves de la ciberseguridad, para predecir, prevenir u obstaculizar las amenazas y/o riesgos emergentes que puedan surgir desde o traves del mismo y que afecten los intereses nacionales, la soberania nacional y su proyeccion a la soberania digital; proyectar y capacitar los recursos humanos necesarios con las capacidades ciberneticas, de manera a contar con las competencias necesarias, para llevar a cabo las actividades a ser desarrolladas en el ciberespacio, a cargo del Ministerio de Defensa Nacional (MDN) y a traves de las Fuerzas Militares (FFMM). (Ciberdefensa, 2021)

Con esta investigacion, se busca orientar al Comando de Operaciones de Defensa Interna (CODI), en su mision de pacificacion y dar respuestas a las amenazas de las operaciones militares desarrolladas, a través de doctrinas, equipamientos y funciones correspondientes para la protección de las informaciones y sus componentes.

La investigación se considera relevante para el Comando de Operaciones de Defensa Interna (CODI), porque se realiza para contribuir para una solución posible a un problema que

crece con rapidez y que redundará en beneficio de la seguridad ante acciones que podrían afectar a la institución.

Ese aspecto, motivó presentar este trabajo para que el Comando de Operaciones de Defensa Interna (CODI), profundice efectivamente tema de ciberdefensa y ciberseguridad en las operaciones militares, de tal manera a realizar su misión de forma más eficaz y segura.

Se considera viable, porque se cuenta con los recursos previstos para su desarrollo y el tiempo necesario para su ejecución conforme al cronograma establecido en el calendario.

Se presentan estadísticas obtenidas a partir de los incidentes cibernéticos reportados y gestionados a través del servicio del año 2020, estos incidentes cibernéticos son reportados por los ciudadanos, funcionarios de gobierno, profesionales independientes y de empresas privadas, CSIRTs extranjeros, etc. o detectados de forma no sistemática. (CERT-PY, 2020)

Los reportes recibidos fueron un total de 2101, de los cuales los incidentes atendidos solo fueron de 1358, pero se realizaron investigaciones en un total de 6598, la mayor cantidad de incidentes investigados son los sistemas o equipos comprometidos, tales como desfiguraciones de sitio web, servidores comprometidos que alojan códigos maliciosos, phishing u otro tipo de artefactos maliciosos, etc. En la mayoría de los casos, el compromiso se debió a páginas web con credenciales débiles (contraseñas fáciles y/o por defecto), en otros casos se debió a páginas web desactualizadas y vulnerables y también sistemas comprometidos por malware. (CERT-PY, 2020)

Para Gabriela Ratti, directora del Centro de Respuestas a Incidentes Cibernéticos de Paraguay (CERT-PY) el aumento en la cantidad de incidentes cibernéticos es sostenido y lineal, en torno al 40% anual, por lo que no podemos atribuir ese aumento a la pandemia. Sin embargo, hubo factores que podrían haber incidido, tales como:

- El COVID-19 fue utilizado por muchos criminales como “gancho” en múltiples engaños o fraudes digitales (phishing, scam, estafas mediante ingeniería social y otros.)

- Muchas personas y organizaciones aumentaron su dependencia de las tecnologías y digitalización, por lo cual tomaron mayor conciencia de su importancia y reportaron los ataques que antes, muchas veces, eran ignorados.

En Paraguay se ha registrado un aumento sostenido de casos de secuestro de cuentas de Whatsapp y de billeteras electrónicas, en su mayoría, mediante ingeniería social (engaños). "Sobre todo, se notó una mayor sofisticación en las técnicas, tanto en los argumentos del engaño como también en los trucos para maximizar el impacto del ataque. Por ejemplo, el bloqueo intencional del mensaje de texto de verificación que, durante 7 horas no permite que la víctima recupere su cuenta, dándole al criminal más tiempo para engañar a los contactos de la víctima y convencerlos de que le transfieran dinero. En los secuestros de cuentas de Whatsapp, extorsiones por redes sociales, etc. cuando deriva en una transferencia o giro de dinero, la gran mayoría de las veces, los atacantes son paraguayos (o al menos se encuentran en territorio paraguayo). De acuerdo a los datos de la Policía Nacional, muchos de este tipo de casos en particular, tienen su origen o vinculación con criminales que se encuentran en las cárceles. (CERT-PY, 2020)

Los conflictos de carácter híbridos, tienen como centro de gravedad (CDG) a la población y a las infraestructuras críticas, que en su mayor parte se encuentra en manos del sector privado a través de servicios en plataformas virtuales desenvolviéndose en el ciberespacio.

Si la nueva forma de guerra, calificada como híbrida, es entendida hoy como la más compleja y, probablemente, la más amplia expresión de la guerra moderna, tanto más es la forma de lograr su victoria. Los aspectos originales de la trilogía de Clausewitz ya no son aplicables, en razón de que la guerra ha pasado de una "contienda de voluntades" a una "empresa mutua" en la que todas las partes se necesitan mutuamente para llevar adelante la empresa de guerra acorde con las necesidades políticas y las alianzas del momento. Además el

pueblo, miembro original de la trilogía de Clausewitz, ha dejado de ser un espectador para pasar a ser un actor casi preponderante en el desarrollo de las acciones. (Locatelli, 2017)

La nueva forma de guerra ha evolucionado hasta entremezclar conductas militares vinculadas a diversos intereses políticos, con terroríficas intenciones afines a necesidades regionales, enmascaradas en cuestiones ideológicas cubiertas de religión. Tanto así que en 2008, el Jefe del Estado Mayor del Ejército de Estados Unidos caracterizó las amenazas híbridas como adversarios que incorporan "combinaciones diversas y dinámicas de capacidades convencionales, irregulares, terroristas y criminales". El antiguo Comando Conjunto de las Fuerzas Armadas de Estados Unidos definió una amenaza híbrida como "cualquier adversario que, simultáneamente y de manera adaptativa, emplea una combinación hecha a medida de medios convencionales, irregulares, terroristas y criminales o actividades en el espacio de batalla operacional. Además, se puede considerar a la amenaza híbrida como una combinación de actores estatales y no estatales. (Locatelli, 2017)

El desarrollo del empleo de ciberdefensa y ciberseguridad, se presenta como una contribución a las operaciones militares del nivel operacional, que tiene entre sus finalidades asegurar la protección de medios como infraestructuras críticas.

Se ha observado que existen un sin números de trabajos de investigación tanto en el ámbito nacional como internacional relacionados a este trabajo de investigacion.

Sobre la regulación de la ciberseguridad en América, durante la Asamblea General de la Organización de los Estados Americanos (OEA) en 2004, los Estados miembros aprobaron la estrategia interamericana integral para combatir las amenazas a la seguridad cibernética; en Paraguay los aspectos legales principales a considerar son el Libro Blanco de la Defensa Nacional, la Política de Defensa Nacional 2019-2030, la Política Militar y la Política de Ciberdefensa, donde se mencionan y abordan en varios apartados lo relacionados a la ciberdefensa y a la defensa del ciberespacio, sin embargo, en el Comando de Operaciones de

Defensa Interna (CODI) no se abordó el tema de manera efectiva y decidida para planificar y ejecutar las acciones relativas a la ciberdefensa militar en las redes y sistemas de información y telecomunicaciones de las Fuerzas Armadas u otros que pudiera tener encomendados, así como contribuir a la respuesta adecuada en el espacio cibernético ante amenazas o agresiones que puedan afectar a la Defensa Nacional.

Formulación del problema

¿Cuál es la importancia de ciberdefensa y ciberseguridad para la protección del ciberespacio dentro del Comando de Operaciones de Defensa Interna (CODI) para las operaciones militares?

Sistematización del problema

Para dar respuesta, a la interrogante principal que constituye el problema de investigación surgen las siguientes preguntas específicas o sistematización del problema: ¿Cuáles son las ciberamenazas que podrían afectar a las operaciones militares del Comando de Operaciones de Defensa Interna (CODI) para determinar las medidas de seguridad de su ciberespacio?; ¿Cómo realizar el empleo de ciberseguridad para determinar las más adecuadas a ser implementadas en las operaciones militares del Comando de Operaciones de Defensa Interna (CODI)?; y ¿Cómo identificar personal y equipos especiales de ciberseguridad y ciberdefensa para ser propuestos al Comando de Operaciones de Defensa Interna (CODI)?

Objetivos

Objetivo General

Analizar la importancia de ciberdedensa y ciberseguridad para la protección del ciberespacio en el marco de las operaciones militares llevadas a cabo por el Comando de Operaciones de Dedensa Intena (CODI).

Objetivos Particulares

Objetivo Específico 1:

Identificar las ciberamenazas que podrían afectar a las operaciones militares del Comando de Operaciones de Defensa Interna (CODI) para determinar las medidas de seguridad de su ciberespacio.

Objetivo Específico 2:

Describir el empleo de ciberseguridad para determinar las más adecuadas a ser implementadas en las operaciones militares del Comando de Operaciones de Defensa Interna (CODI).

Objetivo Específico 3:

Identificar personal y equipos especiales de ciberseguridad y ciberdefensa para ser propuestos al Comando de Operaciones de Defensa Interna (CODI).

Explicación del método

En la investigación fue empleada el método deductivo, para ello se realizaron análisis y descripciones que condujeron a conclusiones parciales durante el desarrollo del trabajo, finalmente se redactó la conclusión general para dar respuesta a los objetivos de investigación planteados.

Diseño de la investigación:

El diseño de la investigación fue el explicativo, debido a que se describió el problema y se intentó responder o encontrar los motivos.

Técnicas de validación:

Las técnicas de validación empleadas fueron:

- Análisis bibliográfico.
- Análisis lógico.
- Entrevista

Cnel DCEM Adolfo Fernández Encina – Sub Director General de la Dirección de Material Bélico (Comandante del Batallón de Inteligencia Militar – BIMI 2017/2019).

Esquema gráfico – metodológico:

Ver anexo 03

Capítulo I

Ciberamenazas que podrían afectar a las operaciones militares del Comando de Operaciones de Defensa Interna (CODI) para determinar las medidas de seguridad de su ciberespacio.

Propósito

El proposito de este capitulo es obtener conclusiones referidas a situación en cuanto a sus efectos, sus protagonistas y su estado actual de ciberamenazas del ciberespacio dentro de las operaciones militares en los departamentos de Concepción, San Pedro y Amambay.

En los antecedentes del problema, de cómo los grupos armados en acciones terroristas o guerrilleras afectan su población y desarrollo; también se agrega a esto las infraestructuras críticas y es importante mencionar que prácticamente son nulas las acciones de protección del ciberespacio por medio de la ciberseguridad y ciberdefensa de las instituciones del estado.

Sección I – Ciberamenazas

Las ciberamenazas, han evolucionados en un ecosistema cada vez más complejo, dinámico, interrelacionado y versátil; tal es así, que los incidentes de violación de la seguridad en el ciberespacio trascienden todos los campos de las expresiones del poder nacional e inciden en la soberanía digital, produciendo vulnerabilidad de las infraestructuras críticas.

Entendida, como las amenazas que se desarrollan en el ciberespacio, son múltiples y heterogéneas, sus potencial daño es mucho mayor que antaño, debido principalmente al crecimiento exponencial de ese espacio cibernético. Las ciberamenazas reúnen una serie de cualidades que incrementan notablemente su peligrosidad, alavés que se dificultan su control y eventual anulación. (Bartolome, n.d.)

La actualidad tecnológica exige un mundo de sistemas complejos e interconectados que traen como consecuencia el crecimiento de las amenazas cibernéticas a ritmos exponenciales y a velocidades desconcertantes. En este contexto, la Ciberdefensa toma un papel preponderante

que involucra diversos actores, dándole el eje fundamental a las Fuerzas Militares, para proponer una visión que asegure la defensa cibernética nacional, así como la resiliencia y continuidad de las Infraestructuras Críticas. (Cano, 2018)

Por su parte, la convergencia tecnológica, la densidad digital, los productos y servicios digitalmente modificados, entre otros, han incrementado los niveles de riesgo cibernético nacional. En este contexto, se revela que estamos frente a una serie de retos que exigen altos niveles de dependencia tecnológica, que despliega un escenario de oportunidades, pero también complejo y desafiante de cara al crecimiento exponencial de las amenazas y vulnerabilidades cibernéticas a la Ciberdefensa Nacional. (Ciberdefensa, 2021)

Por su parte, la convergencia tecnológica, la densidad digital, los productos y servicios digitalmente modificados, entre otros, han incrementado los niveles de riesgo cibernético nacional. En este contexto, se revela que estamos frente a una serie de retos que exigen altos niveles de dependencia tecnológica, que despliega un escenario de oportunidades, pero también complejo y desafiante de cara al crecimiento exponencial de las amenazas y vulnerabilidades cibernéticas a la Ciberdefensa Nacional. (Cano, 2018)

Sección II – Amenazas actuales en el ciberespacio

Anualmente, se publican estudios e informes que analizan el panorama global de las ciberamenazas y sus tendencias. En estos estudios se mezclan fuentes de ciberamenazas (estados, terroristas, ciberactivistas, etc.) con tipos de ciberataques (phishing, ataque DNS, etc.) y objetivos (dispositivos móviles, cadena de suministro, informaciones falsas, robos de credenciales, etc.) y se analiza la información desde diferentes puntos de vista. (Ganuza, 2020)

De acuerdo con el informe de "ciberamenazas y tendencias del CERT Gubernamental español (CCN-CERT)" de 2019, las ciberamenazas más significativas del panorama internacional son los Estados y los grupos patrocinados por ellos; siendo otras ciberamenazas relevantes los ataques a la cadena de suministros, las acciones en el ciberespacio de grupos

terroristas, yihadistas y ciberactivistas, las noticias falsas, así como los ataques contra los datos personales (con el fin último de cometer ciertos delitos, robar credenciales, suplantación de identidad o espionaje). (Ganuza, 2020)

El informe de CheckPoint (cyber attack trends: 2019 mid-year report) refleja un panorama diferente, o con otro punto de vista, haciendo hincapié en el aumento de cuatro tipos de ataques con respecto al año anterior (ataques a la cadena de suministro de software, estafas cada vez más sofisticadas a través de emails, ciberataques a recursos en la nube y ciberataques a dispositivos móviles) y en la persistencia de otros tres tipos de ataques (ransomware, criptominado48 y ataques DNS49). (Ganuza, 2020)

Para afrontar adecuadamente las amenazas cibernéticas, es imprescindible el fortalecimiento de la cooperación judicial y policial internacional, articulando los instrumentos adecuados de colaboración e intercambio de información y la armonización de las legislaciones nacionales, con el desarrollo y mantenimiento de una regulación sólida y eficaz. En concreto, este Plan Nacional promoverá la ratificación del Convenio de Budapest y la creación de leyes adicionales para la ejecución de sus compromisos en virtud de dicho Convenio. (MITIC, 2017)

Sección III – Ciberamenazas a redes y sistemas del ámbito de la defensa

Tanto en tiempos de paz como durante el desarrollo de operaciones de las fuerzas militares, los sistemas informáticos empleados y las redes que eventualmente se integran, están sujetas a las mismas amenazas enunciadas en este capítulo. La cantidad de sistemas y redes empleadas por una fuerza está en relación directamente proporcional con el nivel de desarrollo tecnológico del Estado al cual pertenecen, a mayor nivel de desarrollo, mayor cantidad de sistemas y redes, es más grande la cantidad de blancos que presentan frente a ciberamenazas. (Caceres, 2019, p. 33)

Un breve análisis de los anteriormente mencionado, permite concluir acerca de las múltiples posibilidades de impregnación en las distintas redes a las que un solo individuo accede y emplea de forma diaria a través de las aplicaciones de celular.

Wireless mesh networks (Redes Inalámbricas - WMN), las redes de malla inalámbricas son circuitos ad hoc de conectividad inalámbrica en los que solo un dispositivo requiere una conexión a Internet. Estas son redes inteligentes de dispositivos inalámbricos que se pueden formar, dispersar y reformar según el comando del usuario. Las WMN se crean de abajo hacia arriba mediante conexiones entre dispositivos, sus capacidades de auto formación y auto curación aseguran una comunicación robusta y confiable en cualquier lugar a bajo costo y sin infraestructura fija. Las WMN amplían la informática generalizada integrada en el IoT (Internet of Things – Internet de las cosas) haciéndolo más dinámico. Esta tecnología ofrece múltiples beneficios, entre los más significativos están: la innovación y menor costo, al tiempo que los contras se consolidan en que no existe sistemas de regulación para controlar este tipo de tecnología y con ello se integran un sin número de delitos cibernéticos. (Cano, 2018)

Pervasive Computing (Computación Omnipresente), también conocida como computación ubicua, la cual brinda información, medios, contexto y poder de procesamiento, sin importar la ubicación. Esta clase de tecnologías se caracteriza por amplias redes de microprocesadores conectados o incrustados en objetos cotidianos, los datos se integran y se intercambian en las redes públicas. La computación omnipresente es la tecnología que impulsa Internet de las cosas (IoT), pero es más preciso pensar en ella como el motor de todo el internet. Las capacidades de información, intercambio y colaboración de estas redes no se limitan a ningún dispositivo o ubicación fija; se distribuyen por todo el mundo. Además, el factor de forma de la informática dominante puede ser móvil, usable o implantable. (Cano, 2018)

La ciberdefensa es fundamental para la conducción de las operaciones militares modernas. La infraestructura cibernética militar actual presenta posibles puntos únicos de falla

para las operaciones, el entrenamiento y las actividades. La libertad de acción dentro y a través del ciberespacio depende de nuestra capacidad para proteger y defender contra acciones accidentales, maliciosas o adversarias. (Ganuza, 2020)

Hoy en día, existe una dependencia a nivel global de las computadoras y las redes fácilmente disponibles para la mayoría de los aspectos gubernamentales, financieros, comerciales, industriales, así como, para el mando y el control de las operaciones militares - una dependencia que ha generado grandes oportunidades y riesgos significativos. (Ganuza, 2020)

Ciberamenazas y el riesgo del conflicto armado preventiva

Los mayores problemas planteado a las naciones con capacidades de defensa cibernética reducidas, es la posibilidad de verse envueltos en conflictos con otros países más poderosos, por no poder garantizar la seguridad de sus servidores locales y convertirse en meras plataformas de lanzamiento de armas cibernéticas. (Baretto, 2017)

El uso de forma creciente de las TIC y de los sistemas integrados al Internet en los servicios esenciales, puede representar un aumento de riesgo de ataques cibernéticos. En especial, si la implementación de las TIC en las infraestructuras no está acompañada de medidas de seguridad. El reto de la optimización en la prestación de los servicios esenciales y la conquista de mayor eficiencia y efectividad, se acompaña del desafío del avance en la protección y seguridad de las infraestructuras TIC. (MITIC, 2017)

El conflicto así generado, puede devenir o convertirse en lo que se denomina convencionalmente guerra preventiva. (Caceres, 2019, p. 36), estas son las acciones llevadas a cabo por un Estado contra otro Estado o actor no estatal, que amenaza los intereses vitales del primero.

Normalmente, su empleo no es novedoso, registrándose en la historia militar numerosos ejemplos; la guerra preventiva, aunque no definida por el derecho internacional, es en la

actualidad una práctica de uso común, generalmente reservada a países con un poderío militar importante. (Caceres, 2019)

Sin embargo, es a partir de la difusión de la US National Security Strategy 2002 (NSSR 2002), en donde el concepto retoma vigencia internacional, originando críticas y adhesiones. Presentada por el gobierno del presidente George W Bush, el 17 de septiembre de 2002, expresa: "Si bien Estados Unidos tratará constantemente de obtener el apoyo de la comunidad internacional, no dudaremos en actuar solos, en caso necesario, para ejercer nuestro legítimo derecho a la defensa propia, con medidas preventivas contra esos terroristas, a fin de impedirles causar daños a nuestro pueblo y a nuestro país". Agrega a continuación que "Estados Unidos ha mantenido largamente la opción de acciones preventivas para contrarrestar una amenaza suficiente a nuestra seguridad nacional. Cuanto más grande sea la amenaza, más grande es el riesgo de la inacción y es más necesaria la razón para tomar medidas preventivas para defendernos, incluso aunque sea incierto el momento y el lugar del ataque enemigo. Para impedir o evitar tales actos hostiles de nuestros adversarios, Estados Unidos actuará preventivamente, si es necesario. (Baretto, 2017)

Las operaciones de guerra preventiva, son las acciones llevadas a cabo por un Estado contra otro Estado o actor no estatal, que amenaza a los intereses vitales del primero. Normalmente se inicia sin declaración de hostilidades, aunque puede estar precedida por una serie de advertencias, notificaciones y ultimátums para influir en la decisión de quien será atacado y modifique su conducta respecto a lo que constituye la amenaza. Su empleo no es novedoso, registrándose en la historia militar numerosos ejemplos. (Baretto, 2017)

Caracterización de las amenazas en ciberdefensa

Amenazas internas: Generalmente estas amenazas pueden ser más serias que las externa; los usuarios o personal técnico, conocen la red y saben cómo es su funcionamiento,

ubicación de la información, datos de interés, etc. Además, tienen algún nivel de acceso a la red por las mismas necesidades de su trabajo, lo que les permite unos mínimos de movimientos.

Amenazas Externas: Se originan fuera de la red local, al no tener información certera de la red, un atacante tiene que realizar ciertos pasos para poder conocer qué es lo que hay en ella y buscar la manera de atacarla.

Amenazas por el efecto: El tipo de amenazas por el efecto, que causan a quien recibe el ataque podría clasificarse en: robo de información, destrucción de información, anulación del funcionamiento de los sistemas o efectos que tiendan a ellos, suplantación de la identidad, publicidad de datos personales o confidenciales, cambio de información, venta de datos personales, robo de dinero, estafas, etc.

Por esta razón, los países industrializados que están a la vanguardia en tecnología, como Estados Unidos de Norteamérica (EE.UU.), Rusia, China entre otros, buscan ostentar el dominio del ciberespacio, tanto para el ataque como para la defensa; teniendo en cuenta que el factor tiempo en ciberespacio proporciona un intervalo desde un par de minutos hasta unas milésimas de segundo para realizar un ataque. (Caro Bejarano, 2011)

La propuesta de la Estrategia Militar de Ciberdefensa es una respuesta efectiva a los riesgos y amenazas a los que se ve enfrentada la Seguridad y Defensa del país de cara a las tecnologías disruptivas, con ello, se planteó un modelo sistémico basado en objetivos estratégicos analizados en cada uno de los componentes del Modelo DOMPILEN. Con esto fue preciso delimitar y definir prospectivamente hacia donde deben ir las Fuerzas Militares a fin de desarrollar capacidades militares para el desarrollo de Operaciones Cibernéticas, soportadas en un marco legal y constitucional. (Cano, 2018)

Reto operativo militar

Del análisis realizado por el Departamento de Ciberseguridad de la Dirección General de Tecnologías de la Información y Comunicación de las Fuerzas Armadas de la Nación,

actualmente encargada de los estudios para las propuestas de ciberdefensa y ciberseguridad militar, se extrae que el entorno operativo actual, así como el previsible entorno futuro y las implicaciones que de él se derivan para las capacidades de las FF.AA. y del Ministerio de Defensa Nacional, en general, constituyen la base sobre la que se fundamentan las acciones de ciberdefensa.

Se considera un entorno global y dinámico, en constante evolución sobre un escenario complejo con características propias que favorecen la actuación del atacante a las operaciones militares, ámbito ligado al espectro electromagnético y transversal.

Las acciones que se realizan en él, pueden causar importantes efectos sobre el correcto funcionamiento de las infraestructuras críticas y servicios esenciales del país.

El reto de la optimización en la prestación de los servicios esenciales y la conquista de mayor eficiencia y efectividad, se acompaña del desafío del avance en la protección y seguridad de las infraestructuras TIC. En este contexto, es esencial que Paraguay defina cuáles son sus infraestructuras críticas en términos de ciberseguridad, es decir, las infraestructuras críticas que utilizan TIC y sistemas integrados al Internet para su operación. Así, se debe realizar un estudio sobre las condiciones de seguridad de estas infraestructuras, tanto del sector público como del sector privado; establecer normas claras, protocolos y un plan de comunicación nacional para proteger la infraestructura crítica en el caso de un ataque cibernético. (MITIC, 2017)

Operadores de infraestructuras críticas deben llevar a cabo periódicamente las mejores prácticas en ciberseguridad, tales como evaluaciones para identificar las vulnerabilidades de seguridad en las computadoras, las redes y la infraestructura de comunicación, así como los mecanismos para hacer frente a estas vulnerabilidades.

En este contexto, la ciberdefensa toma un papel preponderante que involucra diversos actores, dándole el eje fundamental a las Fuerzas Militares, para proponer una visión que asegure la defensa cibernética nacional, así como la resiliencia y continuidad de las

Infraestructuras Críticas Cibernéticas, en el quinto dominio de la guerra: el ciberespacio. Por su parte, la convergencia tecnológica, la densidad digital, los productos y servicios digitalmente modificados, entre otros. En este contexto, se revela que estamos frente a una serie de retos que exigen altos niveles de dependencia tecnológica, que despliega un escenario de oportunidades, pero también complejo y desafiante de cara al crecimiento exponencial de las amenazas y vulnerabilidades cibernéticas a la Ciberdefensa Nacional. (Cano, 2018)

Se debe agregar que, como lo afirma el autor Schwab Klaus, la revolución digital en su esencia, "No cambia lo que hacemos, sino que cambia lo que somos", lo que marca un inicio para repensar y evolucionar el concepto de la Defensa Nacional al nuevo entorno operacional llamado ciberespacio, con el fin de comprender la dinámica de las vulnerabilidades y los retos ante la nueva revolución digital. En este nuevo dominio, es posible que un ataque cibernético realizado a las plataformas tecnológicas que soportan los servicios esenciales brindados a la población debilite o impida la gobernabilidad de un país, imposibilite la prestación de servicios esenciales ocasionando sufrimiento y, en otros casos, la muerte e incluso desequilibre la economía; hechos que en conjunto pueden desestabilizar la Seguridad y Defensa Nacional. (Cano, 2018)

El campo de la ciberseguridad ha despertado el interés de la academia y teóricos de las relaciones internacionales, siendo el paradigma neorrealista, constructivista, así como la teoría de la guerra, las que han promovido la noción del ciberpoder y los vínculos de la problemática del ciberespacio con la seguridad nacional y la política exterior. En ese sentido, destaca cómo en la última década las amenazas y riesgos provenientes del ciberespacio se han incrementado a un ritmo acelerado, transformando a la ciberseguridad en un tema central de la política de seguridad nacional, así como factor de trascendencia de la política exterior de los Estados. (Antonio, 2021)

Sección IV – Ciberdefensa

Uno de los aspectos más importantes en la ciberdefensa es la protección de las infraestructuras criticas nacionales frente a ciberamenazas.

La protección es responsabilidad de los operadores que proporcionan el suministro habitual en periodos de paz o estabilidad, la preestablecida por los operadores no suele ser suficiente para protegerse frente a ciberataques sofisticados, de modo que para generar medidas adicionales que compensen las carencias en los casos de extrema gravedad pueden ser en forma de previsión y reserva de recursos económicos o humanos adicionales.

La fuerza del ciberespacio debe estar preparada, en caso de necesidad nacional, para prestar apoyos puntuales a los operadores críticos que se determinen, mediante el empleo de sus capacidades operativas y técnicas; en especial, su capacidad de gestión de eventos de seguridad, auditorías, investigación forense digital y ciberdefensa desplegable.

Son muy habituales las acciones de desinformación con la finalidad de cambiar la opinión de un público objetivo sobre un asunto concreto, reemplazándola por otra visión alternativa; y son consideradas por los poderes políticos como uno de los grandes problemas a resolver.

Dentro del marco de competencia de la República del Paraguay, existe legislación suficiente referida a la ciberdefensa, a partir de la Ley N˚4989 del año 2013 “Que crea el Marco de Aplicación de Tecnologías de la Información y Comunicación en el Sector Público y crea la Secretaría Nacional de Tecnologías de la Información y Comunicación (SENATICs)”, se crea la institución del Poder Ejecutivo encargada de implementar los principios y fines de las TIC en el sector público. Conforme lo dispone la referida Ley, la investigación, el fomento y el desarrollo de las TIC son una política de Estado que involucra a todos los sectores y la sociedad. Las TIC deben servir al interés general y es deber del Estado promover su acceso de manera eficiente y en igualdad de oportunidad a todos los ciudadanos. Siendo así, la SENATICs es la

institución del Poder Ejecutivo que define, fiscaliza y apoya la implementación de políticas y estrategias transversales para garantizar el acceso y el uso de las TIC a la población paraguaya con el fin de mejorar su calidad de vida y apoyar el desarrollo sostenible del país. Para lograrlo, una de las líneas de acción en las que trabaja es el Gobierno Electrónico, ofreciendo servicios de hosting, ingeniería en TIC, asistencia técnica, implementación de portales, computación en la nube, automatización de trámites, aplicaciones ciudadanas, capacitaciones, trámites en línea, entre otros numerosos servicios. (MITIC, 2017)

Aun así, todavía se encuentra en proceso de desarrollo y expansión regulativa. Su organización se basa sobre una estructura burocrática y formal en la que actualmente orienta su desarrollo a la ejecución de tareas de carácter especializado que se realicen en áreas específicas, sobre una conducción basada en una cadena de mando que integre los poderes del Estado y a una toma de decisiones cada vez más centralizada. Por otra parte, el poder militar ha ido encontrando un espacio para el empleo de sus capacidades dentro del ciberespacio, tras continuas modificaciones y producto de las politicas variables.

Sección V – Ciberamenaza en el Comando de Operaciones de Defensa Interna (CODI)

En las operaciones militares, existen diversas ciberamenazas que pueden afectar la seguridad y el funcionamiento del Comando de Operaciones de Defensa Interna (CODI), algunas de las principales ciberamenazas en este ámbito son las siguientes:

Ataques cibernéticos a la infraestructura de defensa: Esto incluye ataques dirigidos a sistemas de comunicación, redes de comando y control, sistemas de armas y otros activos militares críticos. Los ciberatacantes pueden intentar interrumpir o desactivar estas infraestructuras, lo que podría tener un impacto significativo en la capacidad operativa de las fuerzas armadas.

Espionaje Espionaje y robo de información: Los ciberespías y actores estatales pueden tratar de infiltrarse en redes militares para obtener información clasificada, secretos de defensa

y equipos estratégicos. El robo de información confidencial puede socavar la seguridad de las operaciones y proporcionar ventajas tácticas a los grupos armados al margen de la ley.

Malware y ransomware: El malware y el ransomware son formas comunes de ciberataques que pueden afectar a las operaciones militares. El malware puede infectar sistemas y redes, permitiendo a los atacantes controlarlos, robar información o interrumpir su funcionamiento normal. El ransomware cifra los archivos y exige un rescate para su liberación, lo que puede afectar la disponibilidad y confidencialidad de la información crítica.

Ataques de denegación de servicio (DDoS): Los ataques DDoS buscan saturar los recursos de red o sistemas específicos, impidiendo que los usuarios legítimos accedan a ellos. En el contexto militar, estos ataques pueden utilizarse para obstaculizar las comunicaciones, interrumpir el comando y control, o afectar el funcionamiento de los sistemas de armas.

Ingeniería social y ataques de phishing: Los ciberdelincuentes pueden utilizar técnicas de ingeniería social para engañar a los usuarios y obtener acceso a sistemas militares. Los ataques de phishing buscan obtener credenciales de acceso o información confidencial a través del engaño, como correos electrónicos falsos que parecen legítimos.

Amenazas internas: Las fuerzas armadas también deben considerar las amenazas internas, es decir, el riesgo de que el personal militar o contratistas malintencionados puedan abusar de su acceso privilegiado para causar daño o filtrar información sensible.

Vulnerabilidades en sistemas de armas y plataformas: Los sistemas de armas modernos están cada vez más interconectados y dependen de la tecnología. Las vulnerabilidades en el diseño o implementación de estos sistemas pueden permitir a los adversarios tomar el control o sabotear su funcionamiento.

Estas son solo algunas de las ciberamenazas más comunes en las operaciones militares, es importante destacar que el panorama de amenazas evoluciona constantemente, por lo que el Comando de Operaciones de Defensa Interna (CODI), debe estar preparada para enfrentar

nuevas formas de ciberataques y consolidarse actualizados en términos de medidas de ciberseguridad y defensa cibernética.

Para que una fuente sea considerada una ciberamenaza debe cumplir tres requisitos: capacidad, interés y animosidad. Debe tener la capacidad de identificar y aprovecharse de las vulnerabilidades de las redes y sistemas TIC de la víctima y de llegar a causarles un efecto pernicioso. Debe tener interés en los activos de la víctima, en especial la información debe tener valor rentable para la fuente de amenaza, de tal manera, que los beneficios esperados compensen el gasto de los recursos necesarios para realizar el ciberataque. Por último, debe tener animosidad contra la potencial víctima, es decir, interés en causar perjuicio a sus redes y sistemas TIC, aunque no le aporte un beneficio directo, sino una ventaja operativa en el marco de un conflicto o una ventaja competitiva en un entorno comercial. (Ganuza, 2020)

La amenaza a las tecnologías de la información nunca ha sido mayor y los usuarios necesitan y demandan seguridad como nunca antes había ocurrido. Los ataques pueden ser procedentes no sólo de hackers informáticos sino de terroristas, organizaciones criminales y extremistas políticos, movimientos fanáticos religiosos, servicios de inteligencia y fuerzas militares adversarias. (Duran, 2011)

La Junta Interamericana de Defensa (JID), apoyada por la Fundación Interamericana de Defensa (FID), ha recibido ciertos mandatos por parte de la Organización de Estados Americanos (OEA) respecto a ciberdefensa, por lo que hemos dado los primeros pasos para generar progresos significativos con la intención de facilitar la comunicación y la colaboración en ciberdefensa entre la fuerzas armadas y de seguridad del Hemisferio Occidental. Al ser la organización que encabeza los asuntos militares y de defensa en las Américas, la JID cuenta con la coyuntura ideal para impactar de manera significativa políticas y estrategias, así como, facilitar una mayor cooperación regional. La JID tiene una posición única para reunir a los tomadores de decisiones tanto militares como civiles de América Latina y el Caribe, con la

finalidad de mejorar el papel de las instituciones militares y de defensa en el aumento de la ciberseguridad, así como, para mejorar la capacitación y el intercambio de información. (Ganuza, 2020)

Se pueden apreciar las ciberamenazas, desde dos enfoques diferente común por su interacción en el ciberespacio, primero en afectar las operaciones militares y las infraestructuras críticas en su área de responsabilidad, la ciberdefensa debe minimizar el riesgo de la exposición y contrarrestar eventos que afecten la libre disponibilidad del ciberespacio en las operaciones militares que realice el instrumento militar en cumplimiento de la normativa vigente en materia de Defensa Nacional. Pueden presentarse como ataques a servidores militares del Comando de Operaciones de Defensa Interna (CODI).

Existen varios objetivos institucional que deberian ser considerados en las operaciones militares realizadas y tambien considerar a las infraestructuras críticas del área de responsabilidad que podría tener consecuencias a nivel nacional.

En la entrevista realizadas al ex comandante del Batallon de Inteligencia Militar (BIMI), Cnel DCEM Adolfo Fernández Encina y actualmente Sub Director General de la Dirección de Material Bélico (DIMABEL), menciona que para afianzarse progresivamente las Fuerzas Militares debe tener la capacidad de proteger la infraestructura critica propia y de todo el Estado. Que actualmente la gestión y aplicación de la ciberdefensa en el ambito de las operaciones militares se encuentra con falta de equipamientos y que podría ser considerado fundamental al momento de la conformación de un destacamento de ciberdefensa, teniendo en cuenta que el personal capacitado es un factor importante para su funcionamiento.

Sobre las operaciones militares, que pueden afectar el ciberespacio el Comando de Operaciones de Defensa Interna (CODI), por lo sensible de sus operaciones y contar con la mejor infraestructura criticas operativa de las fuerzas armadas en tecnología de inteligencia y comunicaciones, menciona que seguramente debe estar en el interés de varios grupos delictivos

y para tal efecto tiene la imperiosa necesidad de proteger sus sistemas informáticos y de seguridad de la información.

Se le consulto como son abordados estas amenazas actualmente y menciona que se encuentra en una etapa incipiente pero que se debe aplicar acciones para fortalecer el empleo de la ciberseguridad de manera eficiente, protegiendo los activos de gestión de información, capacitación, concienciación sobre las amenazas que existen en el ciberespacio y establecer un protocolo de seguridad con manual de proceso interno para evitar la fuga de información.

Conclusiones parciales

Se ha realizado una descripción de las ciberamenazas dentro de las operaciones militares que pueda afectar la protección a redes y sistemas del ámbito de la defensa, el riesgo del conflicto armado preventiva, las amenazas por el origen militar.

En el ambito militar tiene gran importancia el desarrollo de capacidades relacionadas con las nuevas tecnologias, resaltando la necesidad de desarrollar medidas para mejorar la seguridad ante los ataques de amenzas complejas a la que cualquier sistemas defensivas puede enfrentarse, tanto por su potencial efecto sobre el Comando de Operaciones de Defensa Interna (CODI) y la sociedad misma de los departamentos mencionados para el empleo de elementos de combate de las Fuerzas Armadas de la Nacion.

Se concluye preliminarmente, que existe amplia y variada amenazas dentro de las operaciones militares que puede afectar la protección del ciberespacio, sobre lo cuales se resalta las operaciones y sistemas de la Fuerza de Tarea Conjunta (FTC) y el Batallón de Inteligencia Militar (BIMI), sin dejar de mencionar las infraestructuras criticas de su área de responsabilidad que también deben ser objeto de atención por lo sensible que puede representar que las mismas sean afectadas.

Capítulo II

Empleo de ciberseguridad para determinar las más adecuadas a ser implementadas en las operaciones militares del Comando de Operaciones de Defensa Interna (CODI).

Proposito

El proposito de este capitulo es determinar el empleo de ciberseguridad mas adecuadas para realizar las operaciones militares que tiene como mision el Comando de Operaciones de Defensa Interna (CODI), para la cual tiene varios propósitos fundamentales:

Protección de la infraestructura operaciones críticas: Las militares dependen cada vez más de sistemas de información y comunicación, como redes de computadora, sistemas de control de armas y equipos de vigilancia. La ciberseguridad garantiza la protección de estos sistemas críticos contra amenazas cibernéticas que podrían interrumpir o dañar su funcionamiento.

Salvaguardia de la información y la inteligencia: La ciberseguridad en las operaciones militares busca proteger la información y la inteligencia de las fuerzas armadas. Esto incluye la confidencialidad de los datos, la integridad de la información y la disponibilidad de los recursos de comunicación necesarios para mantener una ventaja estratégica.

Mitigación de ataques cibernéticos: Los ciberataques pueden ser lanzados por actores estatales adversarios, grupos terroristas o hackers individuales. La ciberseguridad se utiliza para detectar, prevenir y reducir estos ataques, fortaleciendo las defensas y reduciendo la exposición a vulnerabilidades en los sistemas militares.

Apoyo a operaciones ofensivas: Además de defenderse contra los ciberataques, la ciberseguridad también se emplea en operaciones ofensivas, como la guerra cibernética. Los especialistas en ciberseguridad militares pueden llevar a cabo operaciones encubiertas en el ciberespacio, infiltrarse en sistemas enemigos y sabotear o recopilar información estratégica.

Garantía de la resiliencia de las fuerzas militares: La ciberseguridad permite a las fuerzas militares mantener la resiliencia y la continuidad de las operaciones en caso de un ciberataque exitoso. Esto implica la capacidad de recuperarse rápidamente de un ataque, restaurar los sistemas comprometidos y mantener la funcionalidad operativa incluso en un entorno cibernético hostil.

En resumen, el empleo de ciberseguridad en las operaciones militares tiene como propósito proteger la infraestructura crítica, salvar la información y la inteligencia, mitigar los ataques cibernéticos, apoyar las operaciones ofensivas y garantizar la resiliencia de las fuerzas militares en el ciberespacio.

Seccion I – **Política y doctrina aplicable a ciberdefensa y ciberseguridad en las operaciones militares.**

Política

Nivel político, coordinado por la Presidencia de la República a través del Ministerio de Tecnologías de la Información y Comunicación (MITIC); nivel estratégico – operacional, a cargo del Ministerio de Defensa Nacional, Comando de las Fuerzas Militares abarca las infraestructuras críticas de la defensa y acciones en el ciberespacio; y el nivel operacional – táctico, actualmente restringida al alcance interno de las Fuerzas Armadas de la Nación.

La ciberdefensa debe garantizar la continuidad de las actividades y servicios en situaciones de contingencia cibernética, para el funcionamiento de las FF AA. y su proyección a las expresiones del Poder Nacional.

Definir las acciones prioritarias en el ámbito de la ciberdefensa a corto, mediano y largo plazo en cuanto a: doctrina, capacitación, RRHH, equipamientos, infraestructuras críticas, conectividad, resiliencia y marco legal.

Los objetivos de la política de ciberdefensa del Paraguay se redactan en base a la intención establecida dentro de la Política de Defensa Nacional de la República del Paraguay

que en su presentación menciona “Esta Política Nacional de Defensa (PND), fue elaborada ante la necesidad de prevenir y combatir eficientemente las nuevas amenazas; tales como el terrorismo, los secuestros, el crimen organizado transnacional, el narcotráfico, los grupos armados ilegales, los ataques cibernéticos, entre otras; sin descuidar las amenazas tradicionales para la República del Paraguay”.

Establecer pautas generales, para el empleo de las capacidades cibernéticas dentro del teatro de operaciones; además, sirve como recurso didáctico para orientar el empleo de la ciberseguridad a las operaciones militares. Proporcionará la visión de como funcionar con las nuevas capacidades a adquirir y las estrategias a adoptar para las acciones en ciberseguridad.

De acuerdo al Plan Nacional de Ciberseguridad de la Republica del Paraguay posee principios orientadores para la formulación e implementación de cualquier política pública de ciberseguridad en Paraguay que son las siguientes:

Proporcionalidad: Las medidas a ser aplicadas deben ser adecuadas, necesarias y proporcionales, respetando los derechos fundamentales, en especial los derechos a la intimidad, privacidad, libertad de expresión y libre asociación, que son la prioridad máxima del Estado. Además, es necesario sopesar las oportunidades y amenazas, asegurando la proporcionalidad de las medidas de protección adoptadas, a fin de que no perjudiquen la promoción de la innovación y el desarrollo de nuevas tecnologías.

Coordinación de esfuerzos y uso eficiente de recursos escasos: Todos los sistemas conectados a Internet son potencialmente vulnerables, así que es importante tener en cuenta que es imposible asegurar un ciberespacio totalmente seguro y confiable. Por ello, se debe adoptar la gestión de riesgo en la implementación de políticas de ciberseguridad, a fin de priorizar y justificar las acciones elegidas. Se reconoce la limitación de recursos, así que se promoverá el máximo aprovechamiento de los recursos disponibles y el adecuado análisis y gestión de riesgo, a fin de priorizar y justificar las acciones elegidas.

Responsabilidad compartida: Todos los integrantes de la sociedad comparten responsabilidades en esta materia, incluyendo al Estado, el sector privado empresarial, la academia, las organizaciones de la sociedad civil y los ciudadanos en general. Todos ellos han de sentirse involucrados en la implementación de este Plan Nacional. Para ello, es necesario la implementación de mecanismos de coordinación, diálogo, trabajo conjunto y fomentando y propiciando la cooperación, participación e integración de las múltiples partes interesadas, capaces de compatibilizar iniciativas y propiciar el intercambio de información y conocimiento.

Desarrollo e innovación: Se reconoce la importancia de la innovación para el desarrollo de una economía digital, lo que demanda un ambiente cibernético seguro y capital humano capacitado en el área de TIC y ciberseguridad.

Cooperación internacional: El carácter transnacional de las amenazas hace que sea esencial promover la cooperación regional y global, ya que muchas de las posibles medidas solo resultaran eficaces si se adoptan internacionalmente con la adecuada cooperación y coordinación entre los gobiernos de los países y organismos internacionales. Así también, para generar espacios de discusión sobre ciberseguridad y gobernanza en Internet en ámbitos supranacionales.

Monitoreo y evaluación: La calidad de las políticas públicas de ciberseguridad requiere un proceso continuo de monitoreo y evaluaciones periódicas. Se incorporará el monitoreo en las políticas públicas de ciberseguridad, con el fin de retroalimentar la gestión de las mismas y corregirlas eventualmente.

Brasil define el empleo del poder militar dentro del ciberespacio, bajo una concepción defensiva que garantiza el ejercicio de su soberanía de manera exclusiva, y previene la posibilidad de futuros litigios a través de la disuasión y la cooperación interestatal. Su sistema contempla acciones defensivas, exploratorias y ofensivas que garantizan la seguridad de sus

intereses nacionales, dejando la ejecución de estas de acuerdo con el nivel de decisión que corresponda. (BARROS, 2022)

Las operaciones en el ciberespacio requieren una doctrina de empleo especifica, acorde a las peculiaridades del combate en ese medio. La exclusividad del combate en este nuevo entorno ha originado que numerosos paises hayan elaborado una doctrina propia e independiente; no obstante, al ser un dominio nuevo y encontrarse en una etapa muy inicial del desarrollo, las ciberoperaciones carecen todavia de la historia y de la experiencia vital necesaria para establecer enunciados de doctrina firmes. (Ortega, 2012)

La doctrina ha de entenderse como un conjunto completo de documentos que faciliten la organización, preparación y empleo de las fuerzas armadas en el ciberespacio. Este conjunto debe incluir como mínimo, la visión sobre la ciberdefensa militar por parte de la más alta autoridad de las fuerzas armadas, el concepto de ciberdefensa, la doctrina de empleo de la fuerza ciberespacial, los procedimientos operativos de cada tipo de ciberoperación, las instrucciones técnicas, guías, recomendaciones y buenas prácticas de las actividades de ciberdefensa y la integración de la ciberdefensa en otras doctrinas consolidadas. (Ganuza, 2020)

La ciberdefensa militar se desarrolla a través de un cuerpo doctrinal que establece normas, criterios, principios, procedimientos, orientaciones, recomendaciones y buenas prácticas sobre el diseño, ejecución y planeamiento de las operaciones militares en el ciberespacio.

Las referencias internacionales en materia de doctrina de ciberdefensa son escasas. La OTAN, habitual referente doctrinal para las naciones aliadas como Paraguay, ha aprobado, recientemente, el estándar OTAN AJP-3.20 “Allied Joint Doctrine for Cyberspace Operations”, el cual describe los conceptos básicos de la ciberdefensa. (Ganuza, 2020)

Las naciones son reacias a compartir sus doctrinas de ciberdefensa, sobre todo en lo referente a las actividades de inteligencia y ofensivas; lo que obliga a las naciones a implicarse en el desarrollo de su propio cuerpo doctrinal de ciberdefensa militar.

Cuando se crea una unidad de ciberdefensa por primera vez, según los expertos a tareves de informaciones de fuentes abiertas inicia con la falta de doctrina consolidada del ámbito ciberespacio y la reducida dimensión de la unidad que hace que se tienda a incluirla en la orgánica de otro ámbito ya establecido, como este caso seria el Comando de Operaciones de Defensa Interna (CODI). Esto, a la larga puede crear confusión y malos entendidos, llegando a considerar las unidades de ciberdefensa como unas unidades que llevan a cabo una función más dentro de los ámbitos civil y obviar su verdadera naturaleza de fuerza responsable de las acciones militares en todo el ámbito de operaciones militares en el ciberespacio.

Para facilitar la organización y el uso de la ciberdefensa como una capacidad militar y para garantizar su integración fluida en la acción conjunta con las capacidades terrestres, marítimas y aéreas, es necesario que la ciberdefensa se rija por los mismos principios doctrinales de guerra tradicionales adaptando a las peculiaridades del ciberespacio y la realidad de la misiones constitucionales del Comando de Operaciones de Defensa Interna (CODI).

La doctrina es generalmente el primer aspecto, ya que a menudo es el más fácil, rápido de actualizar y puede afectar drásticamente el desarrollo de las operaciones. En algunos casos, el impacto de los cambios en los otros componentes no puede realizarse plenamente sin alterar de manera significativa la doctrina. Además, la doctrina también puede servir como base para la evolución, con el fin de establecer los planes y tareas necesarias para alcanzar pacificacion total de la zona norte de la Republica del Paraguay.

Sección II – Ciberseguridad

El modelo de gobernanza de seguridad de la información del Estado, aprobado mediante la Resolución del MITIC Nº 733/2019, la cual establece que todas las instituciones del Estado

deben contar con un área de seguridad de la información, con el objetivo de velar por la seguridad de todos los activos de información en cuanto a confidencialidad, integridad y disponibilidad.

Dicha área debe poder reportar a la máxima autoridad y debe ser independiente de las direcciones de TIC o tecnología, entendiéndose que seguridad de la información y ciberseguridad son áreas transversales, con roles y responsabilidades distintos a tecnología.

Una ciberseguridad nacional sólida necesita una estrategia nacional clara, precisa, realista y práctica, que identifique el estado final deseado para definir un modelo de gobernanza específico donde incluya a todos los actores nacionales, con la misión de facilitar la aplicación de las medidas a través de la provisión de los recursos necesarios y vigilar el cumplimiento de las medidas a través del establecimiento de un sistema de indicadores.

Internacionalmente, existe una definición de ciberseguridad dada por la Unión Internacional de Telecomunicaciones en su Resolución 181, Recomendación UIT - TX.1205 de noviembre de 2010, organismo que en la Conferencia de Guadalajara adoptó la siguiente: "La ciberseguridad es el 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". (Vergara, 2016)

Los activos de la institucion 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 ciber entorno. La ciberseguridad garantiza que se alcancen y mantengan las propiedades de seguridad de los activos de la organización y los usuarios contra los riesgos de seguridad correspondientes en el ciberentorno. (Vergara, 2016)

Para alcanzar una ciberseguridad nacional robusta es necesario fortalecer sus tres pilares (ciberresiliencia, ciberprotección y ciberdefensa), así como mantener una estrecha colaboración y cooperación entre ellos y con sus homólogos internacionales. Una ciberseguridad nacional sólida necesita una estrategia nacional de ciberseguridad clara (expresada en un lenguaje entendible en todos los niveles de implicación), precisa (que establezca unas directrices y medidas eficaces adaptadas a la situación nacional), realista (que establezca objetivos concretos alcanzables) y práctica (que prevea los recursos necesarios para su implementación). Una estrategia nacional de ciberseguridad debe identificar el estado final de ciberseguridad nacional deseado, definir un modelo de gobernanza específico que incluya a todos los actores nacionales principales, valorar los principales ciberriesgos a la seguridad nacional, establecer unas medidas concretas para mitigar los ciberriesgos previstos, facilitar la aplicación de las medidas a través de la provisión de los recursos necesarios y vigilar el cumplimiento y la eficacia de las medidas a través del establecimiento de un sistema de indicadores. (Ganuza, 2020)

En este sentido se entiende la ciberdefensa militar como la capacidad dirigida a la defensa del libre y legítimo ejercicio de todas las actividades del ministerio de defensa en el ciberespacio y, además, es la capacidad principal de la ciberdefensa nacional y uno de los pilares de la ciberseguridad nacional. Aspectos relevantes del ecosistema ciberespacial relacionados con la ciberdefensa son la ciberseguridad nacional, la ciberseguridad internacional, la cooperación público privada, los riesgos de terceros, los ciberriesgos asociados a los estados de pandemia y la información. (Ganuza, 2020)

Uno de los aspectos más importantes en la ciberseguridad es la protección de las infraestructuras criticas del Comando de Operaciones de Defensa Interna y tambien de las instituciones del estado en su zona de responsabilidad frente a ciberamenazas.

La protección de las infraestructuras críticas nacionales es responsabilidad de los operadores críticos (sector privado en su gran mayoría) que proporcionan la ciberseguridad que

ellos consideran apropiada para prestar, sin interrupciones, el suministro habitual en periodos de paz o estabilidad. La ciberseguridad preestablecida por los operadores críticos no suele ser suficiente para protegerse frente a ciberataques sofisticados que afecten a la seguridad nacional por lo que se tienen que prever procedimientos, en el marco de la ciberseguridad nacional, para generar medidas de ciberseguridad adicionales que compensen las carencias en los casos de extrema gravedad. Estos mecanismos de compensación pueden ser en forma de previsión y reserva de recursos económicos o humanos adicionales. (Ganuza, 2020)

Sección III - Empleo de ciberseguridad en las operaciones militares

Con el fin de garantizar un entorno digital seguro, la administración pública elabora directrices para la adquisición de productos y servicios TICS y la estandarización de especificaciones mínimas de seguridad así como la precalificación de proveedores que ofrecen estos servicios y productos, que permitan la prevención de incidentes. Se fomentará en las distintas instituciones de la Administración Pública la creación de unidades especializadas en TIC, que trabajarán de forma conjunta en la implementación del Plan Nacional de Ciberseguridad y con el Coordinador Nacional; en un sistema de trabajo coordinado, para facilitar la difusión rápida y eficaz. (MITIC, 2017)

El Plan Nacional de Ciberseguridad cuenta con un plan de acción que define las líneas de acción para el cumplimiento de los objetivos de largo plazo. Se buscará definir, para la adecuada implementación de este Plan Nacional, los productos inmediatos que se buscan y los resultados intermedios, así como los respectivos indicadores. Es fundamental que los productos inmediatos estén vinculados a los resultados intermedios que, por su parte, deben estar vinculados a los objetivos de largo plazos definidos en el plan. Los indicadores son esenciales no sólo para seguir el progreso de la implementación de este Plan Nacional de Ciberseguridad, sino también para apoyar en la revisión general, asegurándose que alcance sus objetivos de manera eficiente y eficaz. (MITIC, 2017)

El Comando de Operaciones de Defensa Interna (CODI), tiene la misión de asegurar todas las redes de dominio para las operaciones militares y la infraestructura criticas de su comunicación e información global frente a ciberataques. Adicionalmente, tiene la responsabilidad de realizar inteligencia sobre amenazas cibernéticas nacionales por diferentes grupos margen de la ley que tenga interes en dañar la imagen de la institucion y sacar provecho de tal evento, deberá asegurar redes y sistemas de seguridad nacional y militar e investigar los ciberdelitos ocurridos en los departamentos bajo su responsabilidad territorial.

La cantidad de sistemas y redes empleados por una fuerza está en relación directamente proporcional con el nivel de desarrollo tecnológico del estado al cual pertenecen. Y del mismo modo, a mayor nivel de desarrollo y mayor cantidad de sistemas y redes, es más grande la cantidad de blancos que presentan frente a ciberamenazas. Esto no significa en modo alguno que aquellas fuerzas con menor cantidad de sistemas y redes puestos en acción en un teatro de operaciones, lleven ventaja sobre las que poseen mayor cantidad. Por el contrario, incluso aún bajo un riesgo elevado de ciberamenazas, las ventajas que fuerzas altamente informatizadas en el campo de combate, tienen sobre fuerzas no digitales ni aptas para desarrollar operaciones en red, son imposibles de compensar. (Vergara, 2016)

Surge, la necesidad de emplear y proteger el ciberespacio para el apoyo de operaciones militares y otras tareas como las acciones realizadas en tiempos de paz dentro una nacion. Deben entenderse a las acciones en este ambiente, como facilitadoras, multiplicadoras de efectos, apoyos y medios de influencia en función de los objetivos perseguidos. Surge entonces como necesidad, elaborar planes de desarrollo y empleo de medios en el ciberespacio, que incluyan organizacion, mision, medios y doctrina relacionada, la cual deberá contemplar la necesaria integración e interactuación con otras instituciones del estado.

La ciberdefensa es fundamental para la conducción de las operaciones militares modernas. La infraestructura cibernética militar actual presenta posibles puntos únicos de falla

para las operaciones, el entrenamiento y las actividades. La libertad de acción dentro y a través del ciberespacio depende de nuestra capacidad para proteger y defender contra acciones accidentales, maliciosas o adversarias. (Ganuza, 2020)

La ciberseguridad es el fundamento para preservar la libertad de acción en el ciberespacio. Comprende la aplicación de medidas de seguridad para la protección de la comunicación, la información y otros sistemas electrónicos, así como, la información que se almacena, procesa o transmite en estos sistemas para salvaguardar la confidencialidad, la integridad y la disponibilidad. La buena ciberseguridad establece las condiciones para el comando operativo efectivo y el control de las fuerzas militares. (Ganuza, 2020)

Al atacar infraestructuras críticas no solo se pone a prueba el mando militar u organizaciones estatales, las instituciones de carácter privado también son afectadas, tales como banco, proveedores de servicios públicos y transportes. Esto quiere decir, que la seguridad y defensa del ciberespacio tiene implicaciones civiles y económicas y esto lo convierte en un objetivo estratégico de la seguridad nacional, por lo tanto los hombres y mujeres que ostentan tal responsabilidad deben estar intelectualmente preparados para asumir el compromiso de la defensa de un país en el teatro de operaciones del ciberespacio. (Vargas, 2014)

La ciberdefensa militar se desarrolla a través de un cuerpo doctrinal que establece normas, criterios, principios, procedimientos, orientaciones, recomendaciones y buenas prácticas sobre el diseño, ejecución y planeamiento de las operaciones militares en el ciberespacio. (Ganuza, 2020)

Las naciones son reacias a compartir sus doctrinas de ciberdefensa, sobre todo en lo referente a las actividades de inteligencia y ofensivas; lo que obliga a las naciones a implicarse en el desarrollo de su propio cuerpo doctrinal de ciberdefensa militar. (Ganuza, 2020)

En el mundo militar las dos partes del ciberespacio (internet y sistema aislados) son de gran importancia: internet nos proporciona una conectividad global y un acceso masivo a la

información; mientras que los sistemas aislados nos proporcionan un entorno eficaz para manejar información clasificada y para realizar actividades que precisan de un alto grado de confidencialidad y aislamiento.

Estas dos características, conectividad global y aislamiento, no son privativas de cada una de las partes del ciberespacio. Ya que también se pueden crear entornos confidenciales y aislados en internet y se pueden crear redes aisladas con una conectividad grande; pero no son los entornos naturales.

Las dos partes (internet y sistemas aislados) son fundamentales en la ciberdefensa nacional, ya que la conectividad global es imprescindible para un acceso extenso a la información y para la cooperación nacional e internacional, el aislamiento y la confidencialidad son fundamentales en aquellas actividades relacionadas con las operaciones militares y la investigación que realice la inteligencia.

Se puede decir entonces que el ciberespacio es un entorno artificial el cual se desarrolla a través de diferentes herramientas que posee la informática y suele asociarse a la red global o comúnmente denominada internet, pero es aún más amplio y abarcativo. En dicho ámbito se llevan a cabo diferentes operaciones las cuales de acuerdo a su naturaleza pueden catalogarse como defensivas u ofensivas y que debido a su especificidad se las denomina ciberoperaciones. (Miranda., 2016)

Ellas deben entenderse como una herramienta más para la solución de problemas militares dentro del ciberespacio, teniendo en cuenta que en éste, no hay un límite geográfico definido. El teatro de operaciones, entonces estará determinado por las redes globales interconectadas. Si las ciberoperaciones a través de diversos ciberataques, son utilizadas de modo defensivo, las mismas perseguirán detectar, mitigar y neutralizar, el impacto que pueda producir un ataque o bien evitar que cumpla con su efecto para el cual fue dirigido. En cambio,

las que se empleen de modo ofensivo, buscaran actuar sobre centros de gravedad, tratando de afectar a estructuras o infraestructuras consideradas críticas. (Miranda., 2016)

Al centro de gravedad se lo identifica de acuerdo a la siguiente definición como: “La fuente de poder que provee fortalezas o capacidades esenciales para el cumplimiento de los intereses, objetivos y misiones de un actor”. Dichos conceptos son importantes y se deben tener presentes a la hora de definir y priorizar cuales serán catalogadas como infraestructuras militares críticas a ser protegidas contra posibles ciberataques. (Miranda., 2016)

El Comando de Operaciones de Defensa Interna debe ejercer la conducción de las operaciones de ciberdefensa en forma permanente en los tres departamentos mencionados en el decreto presidencial como zona de responsabilidad territorial a los efectos de garantizar las operaciones militares en beneficio de la institucion y de la Defensa Nacional en cumplimiento de su misión principal de acuerdo a los lineamientos establecidos en el Planeamiento Estratégico Militar.

Sección IV – Ciberdefensa y ciberseguridad en el CODI

En tiempos pasados la industria militar era el motor y el referente de una industria civil que aprovechaba los avances de la investigación y desarrollo militar de doble uso en su beneficio. Actualmente la tendencia es la contraria, las grandes corporaciones multinacionales junto con las universidades realizan las grandes aportaciones tecnológicas de las cuales se nutre el estamento militar. Muchas de las tecnologías desarrolladas en el sector de las tecnologías de la información, de la ciberseguridad, de las redes sociales, etc., son de gran utilidad en el campo de la ciberdefensa militar. (Ganuza, 2020)

El Comando de Operaciones de Defensa Interna (CODI) como institucion responsable de los tres departamentos en materia de seguridad interna y desarrollo nacional deberá proporcionar un conjunto de principios para la planificación, diseño, desarrollo y despliegue de capacidades de ciberdefensa. Esta institucion militar tiene un interés directo y apremiante en

reforzar sus capacidades individuales y colectivas de ciberdefensa para garantizar la seguridad de sistemas militares específicos, infraestructura e información, así como, contribuir en asegurar los más altos intereses nacionales contra las crecientes ciberamenazas.

Según el General de Brigada, Comandante de la 3ra Division Canadiense y Fuerzas Conjunta Oeste Stephen M. Lacroix en su escrito en la revista de Ciberdefensa Militar menciona que; “La ciberdefensa es fundamental para la conducción de las operaciones militares modernas. La infraestructura cibernética militar actual presenta posibles puntos únicos de falla para las operaciones, el entrenamiento y las actividades. La libertad de acción dentro y a través del ciberespacio depende de nuestra capacidad para proteger y defender contra acciones accidentales, maliciosas o adversarias. La ciberseguridad es el fundamento para preservar la libertad de acción en el ciberespacio. Comprende la aplicación de medidas de seguridad para la protección de la comunicación, la información y otros sistemas electrónicos, así como, la información que se almacena, procesa o transmite en estos sistemas para salvaguardar la confidencialidad, la integridad y la disponibilidad. La buena ciberseguridad establece las condiciones para el comando operativo efectivo y el control de las fuerzas militares”.

El ciberespacio es físicamente imperceptible, invisible e intangible; esto hace que sea más difícil de entender e interpretar que los ámbitos convencionales. Esta dificultad de comprensión genera una dificultad añadida a la hora de definir y desarrollar capacidades militares, como procedimientos para operar en él ciberespacio es un entorno dinámico y cambiante que obliga a una monitorización continua, a una actualización rápida de la conciencia de la situación ciberespacial (cyber situational awareness) y a una planificación flexible que admita cambios con facilidad. (Ganuza, 2020)

En el contexto de las operaciones militares que realiza el Comando de Operaciones de Defensa Interna (CODI), tanto en ciberdefensa como la ciberseguridad desempeñan roles cruciales para garantizar la seguridad y la eficacia de la institucion. Ambos conceptos trabajan

en conjunto para proteger y mantener la integridad de los sistemas de información y las redes utilizadas en operaciones militares.

La ciberseguridad en las operaciones militares, se enfoca en proteger los sistemas militares de información y las redes contra amenazas cibernéticas, tales como ciberataques, malware, phishing y otras formas de ciberdelincuencia. Su objetivo principal es asegurar la confidencialidad, integridad y disponibilidad de la información y sistemas utilizados en operaciones militares que realiza el Comando de Operaciones de Defensa Interna (CODI). Esto implica implementar medidas de seguridad, como el uso de firewalls, sistemas de detección de intrusiones, cifrado de datos y autenticación de usuarios, entre otros.

La ciberdefensa, va más allá de la ciberseguridad y se enfoca en la preparación, detección y respuesta ante amenazas cibernéticas en el ámbito militar. Esto implica desarrollar planes de contingencia y protocolos para enfrentar ciberataques y llevar a cabo un análisis en caso de incidentes de seguridad. La ciberdefensa también incluye la capacidad de reducir el impacto de los ataques y restaurar rápidamente las operaciones normales después de un incidente.

En el contexto de las operaciones militares, los sistemas de comunicación, comando y control, así como los sistemas de armas y las infraestructuras críticas, están cada vez más interconectados y dependen de la tecnología de la información. Esto hace que la ciberseguridad y la ciberdefensa sean fundamentales para proteger la capacidad operativa del Comando de Operaciones de Defensa Interna (CODI), y para garantizar que la información y los recursos no caigan en manos de adversarios o sean comprometidos por actores malintencionados.

Además, en el ámbito militar, los equipos de ciberseguridad y ciberdefensa también deben estar preparados para enfrentar amenazas específicas y avanzadas, como ataques cibernéticos patrocinados por estados nacionales, espionaje cibernético, sabotaje y desinformación, entre otros. La colaboración con expertos en operaciones de inteligencia,

militares y otros campos es crucial para una ciberdefensa efectiva y una respuesta adecuada a las amenazas cibernéticas en el entorno militar.

Otra dificultad que encuentra la institucion militar es delimitar el empleo militar de los medios, estos ambientes poseen cierta impunidad relativa, debido a la dificultad de identificar los actores. Tambien, el ambiente cibernético es la transversalidad de ambientes operacionales, debido a que, todos ellos desde la perspectiva física y su inmensidad son envolventes de los ambientes operacionales clásicos de conflicto y el ciberespacio es envolvente de la atmósfera.

Sin embargo, el ciberespacio por las características de trabajar en la virtualidad se sitúa en la mente de las personas y por ello lo envuelve todo. Esta característica le da a estos ambientes una transversalidad que eleva la complejidad operacional, no sólo por sus implicancia sino por la conjugación de todas las otras características comunes entre ellos. Las acciones en este dominio están basadas en efectos, por tratarse de un ambiente completamente tecnificado, las acciones tienen resultados tangibles en sus efectos a similitud de las operaciones aéreas, ya que los efectos pueden ser medidos, estudiados y determinados con exactitud. Esto hace que definir el ritmo de batalla y asimilarlo al cumplimiento de objetivos impuestos sea dificultoso por su la forma intangible de alcanzar objetivos concretos. (Cabrera, 2019)

Conclusiones parciales

La falta de doctrina respecto a la ciberdefensa en los diferentes niveles permite al adversario explotar esta vulnerabilidad para desarrollar operaciones de información que modelen la opinión pública. Aspecto que se agrava ante la complejidad del campo de combate moderno, donde los elementos que conforman el nivel táctico tienen un papel trascendental a la hora de concebir un plan táctico. Por tal razón, la determinación del empleo mas adecuado de ciberseguridad en las operaciones militares a ejecutar en el marco de las actividades realizadas por el Comando de Operaciones de Defensa Interna (CODI), adquiere un papel preponderante dentro del proceso de planificación.

Las operaciones militares puedan ser consideradas un objetivo por parte de los diferentes grupos armados al margen de la ley que operan en la zona norte del territorio paraguayo, dicha actividad desarrollada en el nivel tactico y que aún no ha sido profundizado en el ciberespacio como un ambiente donde se ejecutan un desafío cultural para las fuerzas armadas, donde la guerra centrada en redes soporta la capacidad de transformar la información en acción. Por ello, el objetivo general será Estandarizar el empleo de las redes informáticas en las operaciones militares en donde se evidenció la importancia a la hora de desarrollar cualquier mision dentro del marco legal vigente para el empleo de elementos de combate de las fuerzas armadas de la Republica del Paraguay.

La correcta determinación de planes de contingencia y protocolos establecidos, así como la capacidad de llevar a cabo un análisis forense y restaurar las operaciones normales después de un ataque. La colaboración con expertos en operaciones de inteligencia, y otros campos militares es crucial para una ciberseguridad efectiva en el Comando de Operaciones de Defensa Interna (CODI). Además, es importante estar al tanto de las amenazas emergentes y adaptar adecuadamente las medidas de seguridad y estrategias para estabilizar un paso adelante de los adversarios cibernéticos.

de ciberseguridad más adecuadas a ser implementadas en las operaciones militares del Comando de Operaciones de Defensa Interna (CODI), generará efectos que impacten sobre la percepción de la población o el decisor y alteren el proceso de toma de decisiones en todo momento. Estos efectos deben ser acompañados por un marco legal vigente.

Para lo cual debe organizar subunidades alcanzando estas capacidades de ciberdefensa en las operaciones militares desarrolladas, intentar producir acciones para defenderse de estos ciberataques y asi equilibrar el poder de combate tratando de obtener la victoria si es posible antes del despligue de elementos de combate militar.

El personal componentes de la institución, tienen la plena conciencia de que la ciberdefensa más adecuadas a ser implementadas en las operaciones militares del Comando de Operaciones de Defensa Interna (CODI), constituye la capacidad principal a través del cual se debe implementar doctrina de empleo en coordinación con las demas instituciones del estado que poseen responsabilidad en los tres departamentos a traves de sus respectivas insfraestructuras criticas, no siempre una amenaza es responsabilidad de la ciberdefensa militar, la información y la inteligencia que las fuerzas obtienen en el desempeño de sus funciones pueden ser de utilidad para los organismos responsables de la protección.

Se realizó una descripción del empleo de la ciberseguridad y ciberdefensa en las operaciones militares, para el efecto se abordaron aspectos relacionados al ciberespacio con sus características, áreas y ventajas; así mismo sobre la ciberdefensa con el reto operativo militar y sus elementos.

Así mismo se desarrolló la Ciberseguridad con sistemas informáticos, sobre la actual política y doctrina para el uso de la ciberdefensa y la ciberseguridad en las operaciones militares con sus niveles de decisión.

Este análisis general permite mencionar que el empleo de ciberseguridad más adecuadas a ser implementadas en las operaciones militares del Comando de Operaciones de Defensa Interna (CODI), es fundamental para el logro de los objetivos actuales y que actualmente no se aborda como tal para la protección de datos y empleo de herramientas de seguridad en el establecimiento de políticas aplicables.

Capítulo III

Identificar personal y equipos especiales de ciberseguridad y ciberdefensa para ser propuestos al Comando de Operaciones de Defensa Interna (CODI).

Proposito

El propósito de este capitulo es identificar personal y equipos especiales de ciberseguridad y ciberdefensa para garantizar la protección y la integridad de los sistemas de información y redes de una organización frente a las crecientes amenazas cibernéticas. Algunos de los propósitos clave son:

Proteger la información sensible: Los equipos de ciberseguridad y ciberdefensa están encargados de proteger la información confidencial y sensible de una organización, ya sea información gubernamental, militar, empresarial o personal. Esto implica salvarla contra ataques cibernéticos que podrían dañar su confidencialidad, integridad y disponibilidad.

Prevenir y detectar intrusiones: Estos equipos tienen la tarea de identificar posibles amenazas y vulnerabilidades en los sistemas de información. Realice un monitoreo constante y utilice herramientas de detección de intrusos para identificar patrones y comportamientos sospechosos, y así detectar posibles intrusiones o intentos de ataque.

Responder a incidentes de seguridad: Cuando se produce un incidente de seguridad, los equipos de ciberseguridad y ciberdefensa están preparados para responder de manera rápida y eficiente. Su propósito es reducir el impacto del incidente, contener la amenaza, investigar las causas y restaurar la normalidad en los sistemas afectados lo antes posible.

Realizar análisis forenses: En caso de un ciberataque o incidente de seguridad, estos equipos realizan análisis forenses para recopilar pruebas y determinar cómo ocurrió el incidente, qué información pudo haber sido comprometida y quién puede ser el responsable. Esto es importante para llevar a cabo acciones legales y para mejorar las medidas de seguridad en el futuro.

Mantenerse al día con las amenazas emergentes: Los equipos de ciberseguridad y ciberdefensa se mantendrán constantemente actualizados sobre las últimas amenazas y tendencias en el campo de la ciberseguridad. Esto les permite anticiparse a las nuevas técnicas y tácticas utilizadas por los atacantes, y adaptar sus estrategias y medidas de seguridad en consecuencia.

Desarrollar políticas y estándares de seguridad: Estos equipos también participan en el desarrollo y la implementación de políticas y estándares de seguridad cibernética en una organización. Esto implica establecer directrices y mejores prácticas para proteger la información y los sistemas, así como educar y capacitar al personal para fomentar una cultura de seguridad cibernética.

En resumen, el propósito fundamental de contar con personal y equipos especializados en ciberseguridad y ciberdefensa es garantizar la protección de la información, los sistemas y las redes de una organización frente a las amenazas cibernéticas, y responder de manera efectiva a los incidentes de seguridad para minimizar el impacto en la organización.

Sección I – Personal en ciberdefensa en operaciones militares

El personal de ciberdefensa debe considerarse de dedicación exclusiva. La ciberdefensa es una disciplina de una gran complejidad técnica y operativa, que se relaciona con un ámbito de operaciones, por lo tanto, el personal de ciberdefensa debe permanecer toda su carrera militar en ese ámbito para garantizar su eficacia. Debe evitarse por todos los medios considerar al personal de ciberdefensa como un personal de otros ámbitos que con algún tipo de formación pueda ejercer responsabilidades temporales de ciberdefensa.

Para que se tenga la capacidad de respuesta ante incidentes cibernéticos, los países deben estar preparados para responder de manera eficaz a los incidentes de ciberseguridad. Para lograr este objetivo, es esencial formar un equipo nacional de respuesta ante emergencias informáticas. De hecho, los CERTs (Centros de Respuesta ante Incidentes Cibernéticos, CERT

por sus siglas en inglés), hacen mucho más: no sólo son los principales proveedores de servicios de seguridad informática a los gobiernos y ciudadanos, sino que también promueven la sensibilización en ciberseguridad en toda la sociedad. Como se mencionó, el CERT-PY, como el equipo nacional de respuesta a incidentes del Paraguay, ha venido realizando estas actividades: responder ante incidentes cibernéticos, ofrecer capacitación en materia de ciberseguridad, promover campañas de sensibilización sobre ciberseguridad, testing de infraestructuras, entre otras. (MITIC, 2017)

Sin embargo, como se menciona en el plan nacional de ciberseguridad para seguir trabajando en este sentido, es fundamental que el Comando de Operaciones de Defensa Interna (CODI), cuente con las herramientas necesarias, debe contar con recursos humanos suficientes, infraestructura adecuada y una asignación presupuestaria específica que garantice su adecuada operación. En este contexto, es importante que se implementen programas de capacitación orientados al personal, de modo que se desarrolle un grupo de expertos y se garantice la actualización del conocimiento y habilidades de los profesionales, en un área tan dinámica como lo es la ciberseguridad.

También, implementar medidas que posibiliten que el Comando de Operaciones de Defensa Interna (CODI), opere de manera eficiente, esté equipado para determinar rápidamente las amenazas y aplicar medidas para disuadir futuras amenazas para recuperarse de las amenazas existentes. Además de la adecuada infraestructura, necesita de información sobre incidentes cibernéticos que ocurren en el país a traves de las distintas instituciones del estado responsables del mismo para que su trabajo sea más efectivo. En el ámbito de ciberseguridad, el intercambio de información se ha vuelto fundamental para evaluar y garantizar la respuesta y la recuperación ante intrusiones cibernéticas o ataques a diversos sistemas de información.

Para garantizar el intercambio de información eficaz, es de suma importancia la confidencialidad y la protección de los datos que se comparten. Se buscará promover un

ambiente de confianza para el intercambio rutinario de información de comunicaciones críticas sobre amenazas, vulnerabilidades, intrusiones y anomalías relacionadas con la ciberseguridad, así como las contramedidas y mecanismos de recuperación. (MITIC, 2017)

La ciberdefensa nacional consiste en el desempeño integrado de varios organismos, tanto civiles como militares, cada uno con funciones específicas. Las acciones de ciberseguridad deben estar integrados con los procesos de comando y control ya definidos en la doctrina de operaciones de ciberseguridad.

Si bien el contar con modernas tecnologías y políticas orientadas a la ciberdefensa favorecen el dominio o superioridad en un ambiente en un teatro de operaciones, todas ellas deberán encontrarse sustentadas a través de diversas estructuras que contengan personal idóneo y capacitado. Ello demanda la necesidad de contar con personal militar y civil dentro de cada fuerza armada y que este orientado a tareas vinculadas con el ciberespacio, en materia de medidas de seguridad, resguardo y protección de información y el manejo de nuevas tecnologías. (Miranda., 2016)

La amenaza a las tecnologías de la información nunca ha sido mayor y los usuarios necesitan y demandan seguridad como nunca antes había ocurrido. Los ataques pueden ser procedentes no sólo de hackers informáticos sino de terroristas, organizaciones criminales y extremistas políticos, movimientos fanáticos religiosos, servicios de inteligencia y fuerzas militares adversarias; en la zona norte del territorio, especificamente en los tres departamentos mencionados en el decreto presidencial para el empleo de elementos de combate exiten varios grupos criminales trasnacionales proveniente principalmente de Brasil que ingresan al pais a traves de la frontera seca y la complicidad de la fuerza del orden. Por esta razon, la necesidad de coordinación entre las instituciones del estado define la estructura que se organizará para el cumplimiento de la misión, tanto a nivel estratégico, operativo y táctico.

En cualquier operación militar que implique el empleo de componente cibernético, la cooperación y el intercambio de información son factores esenciales para una acción efectiva que hacen que sea esencial establecer y fortalecer alianzas estratégicas con organismos de seguridad cibernética.

De acuerdo a la declaracion del General de Divison Luciano Jose Penna, Presidente del Consejo de Delegados de la Junta Interamericana de Defensa 2020, “Una significativa cooperación regional e internacional ha surgido en torno a la ciberseguridad entre los gobiernos de las Américas durante la última década, sin embargo, gran parte del progreso se ha centrado principalmente en las instituciones civiles. En algunos países, donde las fuerzas armadas y fuerzas de seguridad desempeñan un papel fundamental en la ciberseguridad, el ejército ha participado activamente en el intercambio de información y mejores prácticas con los estados vecinos. Sin embargo, generalmente las fuerzas militares se han mantenido fuera del creciente marco de colaboración regional que ha evolucionado en torno a la ciberseguridad y el cibercrimen en el hemisferio occidental”. (Ganuza, 2020)

El espacio cibernético es un lugar donde prevalece el anonimato, sin embargo las amenazas cibernéticas sofisticadas provienen de organizaciones militares y agencias de inteligencia de otros Estados. De esta manera los gobiernos tecnológicamente avanzados explotan sus ventajas comparativas con relación al resto de los países, desarrollo de ciberoperaciones también está al alcance de actores secundarios o menos desarrollados en su tecnología. Esta problemática requiere adoptar medidas para armar un sistema lo suficientemente resiliente en ciberseguridad que permita neutralizar cualquier amenaza o riesgo que atente contra nuestras infraestructuras críticas y la información de ellas por medio de la Defensa Nacional. (Cabrera, 2019)

La creacion de un destacamento de ciberdefensa para operaciones militares dentro del Comando de Operaciones de Defensa Interna (CODI), seria beneficioso para la institucion

como tal y que tenga trascendencia a nivel Comando del Ejercito para las demas unidades militares de la capital como del interior del pais, que son mas vulnerables en sus insfraestructuras criticas.

La ciberdefensa en el Comando de Operaciones de Defensa Interna (CODI), es como un conjunto de recursos, actividades, tácticas, técnicas y procedimientos para preservar la seguridad de los sistemas de mando y control, la información que manejan, así como permitir la explotación y respuesta sobre los sistemas necesarios, para garantizar el libre acceso al espacio cibernético de interés militar y permitir el desarrollo eficaz de las operaciones militares que realiza y el uso eficiente de los recursos disponibles.

Sección II – Ciberseguridad

Actualmente, según el plan nacional de ciberseguridad del Ministerio de Tecnologías de la Información y las Comunicaciones, se presenta lo que podría constituir acciones de ciberseguridad para el Comando de Operaciones de Defensa Interna.

Con respecto a las acciones aplicables al uso de la ciberdefensa y la ciberseguridad a las operaciones militares, se sugiere en un principio implementar el proyecto que propone una serie de medidas que ayuden a reducir los riesgos en torno a la ciberseguridad, que contenga los aspectos técnicos, jurídicos y de organización que deban realizarse.

Al igual que otras capacidades, las operaciones cibernéticas deben ser optimizadas en todas las fases de las operaciones militares, comprendiendo cómo estas acciones aprovechan la ventaja del punto decisivo, influyen sobre los centros de gravedad operacionales o estratégicos y cómo apoyan la consecución de los objetivos operacionales.

El arte operacional es la forma creativa en que se combinan los elementos del diseño operacional a través de la estructuración eficiente de acciones tácticas en espacio, tiempo y propósito, con un balance entre riesgo y oportunidad, para crear y mantener condiciones necesarias afines al logro de objetivos del propio nivel o del nivel superior de la conducción.

En el nivel operacional resultará de suma importancia armonizar la disponibilidad de recursos para alcanzar fines, e implicará el uso creativo de esos recursos para diseñar caminos o métodos para alcanzarlos. (Vergara, 2016)

En este contexto, se propone avanzar en una dirección que permita al sistema de defensa nacional, a partir de sus competencias jurisdiccionales, contribuir al plan nacional de ciberseguridad en un sentido general o ampliado, coordinando su accionar con otras entidades y jurisdicciones del sector público nacional, a la vez desarrollar y fortalecer las capacidades de ciberdefensa a fin de estar en condiciones de efectuar una defensa indirecta en el ciberespacio contra un agresor interno y externo que pudiera atacar convencionalmente a las operaciones militares del Comando de Operaciones de Defensa Interna (CODI).

Ciberdefensa como el ensamble de todas las acciones defensivas u ofensivas conducidas en el espacio cibernético en preparación o en la planificación y realización de operaciones militares, para asegurar la eficacia de la acción de las fuerzas armadas y el funcionamiento del Ministerio. Ella complementa las medidas de protección de redes, de sistemas y de información con una capacidad de poder operar en el espacio cibernético y una capacidad de gestión de crisis cibernética. (Vergara, 2016)

Para entender la ciberdefensa es necesario aclarar algunos términos. Hay tres términos que siempre se confunden, seguridad informática, ciberseguridad y ciberdefensa. La seguridad informática es la protección de la triada CID (confiabilidad, integridad y disponibilidad de los datos). Datos: redes informáticas y digitales. La ciberseguridad, es una política estratégica nacional que está referido al logro de la protección de las infraestructuras críticas (ICC). Una ICC es una plataforma que provee un servicio esencial para los intereses nacionales. Ejemplo, si yo a traves de un ataque cibernético modifico la fórmula de un medicamento para que sea tóxico puedo llegar a matar gente, si yo rompo los controles de temperatura o presión atmosférica en una central nuclear puedo causar una explosión nuclear como Stuxnet en Irán y

matar gente. Por otro lado la ciberdefensa es el logro de la política nacional de ciberseguridad en las infraestructuras críticas de la defensa nacional, las cuales incluyen las ICC militares y las que se le asignan al Ministerio de Defensa. (Cabrera, 2019)

La ciberdefensa no es una función de los ámbitos de operaciones convencionales; sino una capacidad de combate especializada en el ámbito de operaciones ciberseguridad, por ello es importante que sea comandada por un mando independiente de los otros ámbitos, aun cuando la dimensión de la subunidad de ciberdefensa sea muy reducida.

El personal de ciberdefensa debe considerarse como crítico, operativo, permanente, de dedicación exclusiva y de larga amortización. Además, se debe prestar especial atención, por su gran potencial, a la reserva voluntaria en el campo de la ciberdefensa. El personal de ciberdefensa es un recurso crítico. La base técnica del conocimiento que requiere las tareas de ciberdefensa es de utilidad también en muchas actividades del sector privado. Una parte significativa del personal clave de ciberdefensa, una vez adquirido un nivel de experiencia y conocimientos elevado, va a ser tentado para abandonar las fuerzas armadas e incorporarse a un puesto mejor remunerado en el sector privado. La probable salida de parte del personal más experto obliga a las unidades de ciberdefensa a ser extremadamente cuidadosas y vigilantes con el conocimiento, garantizando que quede siempre documentado y compartido, de tal manera que, si no se puede evitar la fuga de talentos, al menos hay que evitar la fuga de conocimiento. (Ganuza, 2020)

El personal de ciberdefensa debe tener, a todos los efectos, la consideración de personal combatiente. Todas las tareas y responsabilidades relacionadas con las ciberoperaciones en sus tres facetas, defensivas, de explotación y ofensivas, son acciones de combate, a imagen y semejanza de las acciones defensivas, de explotación y ofensivas en los otros ámbitos. (Ganuza, 2020)

La capacidad de ciberdefensa sería el conjunto de sistemas, infraestructuras, personas, medios de apoyo y procedimientos doctrinales, que permiten cumplir con la misión de defender y custodiar las operaciones militares que realiza el Comando de Operaciones de Defensa Interna (CODI), dentro de los procedimientos legales que le permite la ley de Defensa Nacional.

Es lógico, que las capacidades necesarias para implementar adecuadamente la ciberdefensa, son un subconjunto de las capacidades de ciberseguridad; pero llegamos a este punto deberíamos concretar que entendemos por capacidad y acudiendo al RAE obtendríamos que la afección que mejor se ajusta es la que indica que la capacidad es la actitud, talento o cualidad que dispone alguien para el buen ejercicio de algo; pero si hablamos en términos militares, la capacidad es el conjunto de factores que vendría ser sistemas de armas, infraestructuras militares, personal y medios de apoyos logísticos asentados sobre las bases de unos principios y procedimientos doctrinales que pretenden conseguir un determinado efecto militar a nivel estratégico operacional o táctico para cumplir misiones asignadas.

Equipos especiales de ciberseguridad y ciberdefensa

Según la empresa Imagar Solutions Company, sus equipos estan especializados en la protección de sistemas y aplicaciones contra ataques cibernéticos. En este sentido, utilizan una amplia gama de herramientas y técnicas para identificar y mitigar riesgos de seguridad, monitorear la actividad de red y proteger los datos de una organización ya sea civil o militar.

Cuando hablan de los equipos de ciberseguridad se referier a los profesionales que se encargan de desarrollar e implementar diferentes estrategias de seguridad, además de monitorear la actividad de red y detectar y responder a los incidentes y brechas de seguridad.

Mencionan principalmente tres equipos de ciberseguridad a tener como ejemplo y que podria ser consideradas a ser implementadas en el Comando de Operaciones de Defensa Interna (CODI), en función a los diferentes enfoques que utilizan para ejecutar su mision y estos reciben nombres de colores: equipos rojo, azul y morado.

Equipo rojo, también conocido como “equipo de ataque”, los integrantes de este equipo tienen la función de buscar vulnerabilidades, también pueden evaluar la capacidad de una organización para detectar y responder a ataques, lo cual es importante para conocer la efectividad de su capacidad de defensa. Además, pueden proporcionar informes de las debilidades encontradas y recomendaciones para corregirlas.

Su metodología de trabajo se integra dentro del denominado “hacking ético”, ya que su función es la de ponerse en la piel de los hackers para adelantarse a sus ataques. Su objetivo es buscar vulnerabilidades en los sistemas de defensa de la empresa.

Equipo azul, también se conoce como “equipo de defensa”, su objetivo es la protección de los sistemas y aplicaciones de la organización. Para ello emplean herramientas y técnicas para detectar y mitigar ataques cibernéticos, y para fortalecer la seguridad general de una organización. Por ello, el equipo azul realiza tareas como la configuración de políticas de seguridad, la implementación de soluciones de seguridad, la monitorización de la actividad de red y la detección y respuesta a incidentes. Además se encarga de la implementación de medidas de seguridad proactivas, la detección y respuesta rápida a incidentes de seguridad.

Estos equipos también proporcionan una defensa continua mediante la monitorización constante de los sistemas y la realización de actualizaciones y mejoras para mantener a la organización protegida contra nuevas amenazas.

Equipo de ciberseguridad morado, también conocido como “equipo híbrido”, la principal característica del equipo de ciberseguridad morado es su enfoque combinado en la simulación de ataques y la protección de los sistemas y aplicaciones de una organización. Estos equipos trabajan juntos para simular ataques cibernéticos y evaluar la capacidad de la organización para detectar y mitigar estos ataques.

El objetivo principal del equipo de ciberseguridad morado es proporcionar una visión completa de la seguridad de una organización, evaluando tanto la eficacia de las medidas de

seguridad existentes como la capacidad de la organización para detectar y responder a ataques reales. También permite a la organización identificar debilidades y mejorar sus procesos de seguridad, ya que se enfoca en buscar las debilidades antes de que los atacantes malintencionados puedan explotarlas.

Desde sus orígenes esta organización, siempre ha hecho esfuerzos por la protección de sus sistemas de comunicación e información. Sin embargo fue recién en la Cumbre de Praga de 2002, cuando se incluyó por primera vez la problemática de la ciberdefensa en la agenda de la Alianza. La necesidad de incrementar la protección, quedó establecida en la Cumbre de Riga en 2006. (Baretto, 2017)

Para contrarrestar las amenazas cibernéticas y fortalecer la seguridad en línea, se pueden tomar una serie de medidas y buenas prácticas. Aquí hay algunas formas efectivas de contrarrestar las amenazas cibernéticas:

Mantener el software actualizado: Mantén tu sistema operativo, aplicaciones y programas antivirus actualizados con los últimos parches y actualizaciones de seguridad. Esto ayuda a corregir vulnerabilidades conocidas y proteger tu sistema contra amenazas comunes.

Uso de contraseñas seguras: Crea contraseñas fuertes y únicas para todas tus cuentas en línea. Las contraseñas deben ser largas, combinando letras mayúsculas y minúsculas, números y caracteres especiales. Evita usar contraseñas obvias o compartirlas entre diferentes cuentas.

Aplicar autenticación multifactor (MFA): Habilita la autenticación multifactor siempre que sea posible. Esto proporciona una capa adicional de seguridad al requerir un segundo factor de autenticación, como un código enviado a tu teléfono móvil, junto con tu contraseña.

Tenga precaución al hacer clic en enlaces o descargar archivos: Sé cauteloso al hacer clic en enlaces en correos electrónicos, mensajes o sitios web sospechosos. Evite descargar archivos adjuntos no solicitados o provenientes de fuentes desconocidas, ya que podrían contener malware.

Usando una solución antivirus y antimalware: Instala un software antivirus confiable y un programa antimalware en tus dispositivos. Realiza escaneos periódicos para detectar y eliminar cualquier amenaza potencial.

Hacer copias de seguridad de manera regular: Realiza copias de seguridad periódicas de tus datos importantes y guárdalas en un lugar seguro y fuera de línea. Esto te ayudará a recuperarte rápidamente en caso de un ataque de ransomware u otra pérdida de datos.

Estar alerta a los ataques de phishing: Aprende a identificar los ataques de phishing, que generalmente involucran correos electrónicos o mensajes falsos diseñados para engañarte y obtener información confidencial. Evite proporcionar datos personales o financieros a menos que esté seguro de la autenticidad del remitente.

Educación y concienciación: Mantente informado sobre las últimas tendencias y técnicas utilizadas por los ciberdelincuentes. Participa en programas de concienciación en seguridad cibernética y educa a tus empleados, familiares y amigos sobre las mejores prácticas de seguridad en línea.

Proteger la red doméstica: Asegura tu red doméstica mediante el cambio de contraseñas predeterminadas del router, habilitando el cifrado WPA2 o WPA3, y ocultando el nombre de la red (SSID). Además, evita el uso de redes Wi-Fi públicas no seguras y considera el uso de una red privada virtual (VPN) para proteger tus comunicaciones en línea.

Seguir el principio de menor privilegio: Limita los privilegios de acceso en tus dispositivos y cuentas. Utiliza cuentas con privilegios de administrador solo cuando sea necesario y utiliza cuentas de usuario estándar para las tareas diarias.

Dentro de una confrontación convencional normalmente se vela por excluir al personal civil de esta. Sin embargo, con los ataques cibernéticos es prácticamente inevitable pensar que la población civil no va a resultar afectada, es este campo de batalla virtual, que a la hora de la verdad resulta ser más real de lo esperado, no distingue entre instalaciones militares y servicios

vitales para la población, lo cual, provocaría un cataclismo de dimensiones incalculables. Es por esta razón que es importante la capacidad de ataque, pero muchos más la capacidad de defensa para de este modo minimizar la sensibilidad a la hora de recibir un ataque contra infraestructuras críticas y otro tipo de objetivos que se pueden afectar con un ataque cibernético. (Vargas, 2014)

En un mercado como el actual, las organizaciones buscan demostrar confianza a sus clientes y compromiso con la seguridad de la informacion que manejan. Para ello, el hecho de poseer una certificación de algún estándar o norma ISO referente a seguridad supone una ventaja competitiva, ya que es consecuencia de una correcta gestión de los requisitos de seguridad en los procesos de tratamiento de la informacion.

La ciberseguridad es algo que está muy en auge hoy en día, pero ¿a qué se debe?. La creciente cantidad de incidentes y ataques de seguridad relacionados con la información y sistemas informáticos que sufren las organizaciones actualmente hace que la necesidad de tener controles para garantizar la seguridad de dispositivos, redes de comunicación y activos de información sea indiscutible. Es de esta necesidad de donde nace el concepto de ciberseguridad.

Este tipo de ataques tienen por objetivo acceder, modificar o destruir información sensible de las compañías, instituciones militares o instituciones del estado.

La implementación de medidas eficaces de ciberseguridad no es algo sensillo, ya que, debido a la gran cantidad de equipos y tecnologías utilizadas, los ciberdelincuentes siempre encuentran nuevas opciones de llevar a cabo sus ataques. Sin embargo, existe una forma de implementar medidas de protección de datos e información que hace que el procedimiento de implantación de dichas medidas de seguridad informática sea algo más pautado y natural.

Se trata de los estandares y normas ISO relacionadas con la ciberseguridad y seguridad de la informacion. Las normas ISO son estándares desarrollados y publicados por la Organización Internacional de Normalización (ISO). Tanto ISO como IEC (la Comisión

Electrotécnica Internacional) son la referencia especializada para la normalización a nivel mundial. A través de comités técnicos formados por los organismos miembros tanto de ISO como de IEC, se elaboran normas internacionales redactadas con el objetivo de regularizar procesos específicos sobre ámbitos tales como la seguridad de la Información. (Martin, 2022)

Estas normas constituyen, hoy en día, un elemento indispensable en el sistema de cumplimiento de las organizaciones, otorgando prestigio y reconocimiento internacional a las mismas. El valor diferencial que aportan las implantaciones de las normas ISO a las organizaciones frente a sus competidores se debe a que dichos estandares certificados son revisados y auditados periodicamente para garantizar su cumplimiento, haciendo que la apreciación del nivel estrategico politico mejore considerablemente.

Las normas ISO se numeran de forma incremental en función de su propósito y se dividen en familias para agrupar aquellas que traten aspectos de la misma índole. El objetivo de estos estándares y normas es identificar técnicas, políticas, guías, capacitación, etc. en referencia a su propósito (seguridad, continuidad, calidad, entre otros).

Entre las ya mencionadas normas ISO, destaca la familia ISO 27000. Ésta es una serie compuesta por varias normas de seguridad de la información que detallan las pautas y requisitos para implementar un Sistemas de Gestion de Seguridad de la Informacion (SGSI), con el objetivo de gestionar la seguridad de la información de las organizaciones. Dentro de este conjunto de normas, la principal es la ISO 27001, la referencia certificable de toda la serie. Esta norma proporciona requisitos para el establecimiento, implantación, mantenimiento y mejora continua de un SGSI. El proceso de mejora continua se basa en el conocido ciclo deming o PDCA (de las siglas de las palabras en inglés Plan-Do-Check-Act) que consta de las 4 fases de Planificar, Hacer, Verificar y Actuar. (Martin, 2022)

Conclusiones parciales

Se ha hecho una identificación del personal y equipos especiales de ciberseguridad y ciberdefensa para ser propuestos al Comando de Operaciones de Defensa Interna (CODI), en operaciones militares y la posibilidad de la creacion de un destacamento de ciberseguridad, se mencionan las diferentes fases que deben realizarse de manera institucional de las acciones para el buen desarrollo del tema mencionado.

El primer paso hacia la instauración de buenas prácticas de ciberseguridad es garantizar que el Comando de Operaciones de Defensa Interna (CODI), cuente con personal capacitado en ciberseguridad y que ese personal sea permanente en el sector. Para ello, el aprendizaje sobre ciberseguridad desde los primeros niveles de la enseñanza es importante para fomentar el interés profesional de los Oficiales y Suboficiales que tengan talentos en esta área, y por eso es esencial captar su interés en el tema e identificar a ese personal desde muy temprano en las unidades de enseñanzas de tal manera que participen de forma positiva en la construcción profesional más conectado de modo a tener un ciberespacio seguro y confiable.

Se realiza una mención, que por las características especiales del Comando de Operaciones de Defensa Interna (CODI), por las misiones que cumplen, que la misma puede y debe realizar operaciones militares a traves de acciones de ciberseguridad por sí misma en función a sus activos críticos, de su entorno y así también apoyar a las infraestructuras críticas de su área de responsabilidad.

Conclusiones Finales

No es fácil integrar los esfuerzos gubernamentales, militares y civiles a fin de lograr el objetivo común de proteger el ciberespacio, en la coincidencia de criterios que aparecen como sinónimos entre ciberdefensa y ciberseguridad que apuntan a ella como eje central de la política de seguridad nacional.

Las diferentes acciones llevadas a cabo hoy por la institución exigen una consideración especial por la sensibilidad de sus estructuras de comunicación, planificación, servidores centrales, bases de datos y el interés que pueden generar hacia los mismos las organizaciones criminales, a medida que los resultados actuales de sus acciones trascienden y afectan a todos los estratos criminales en los departamentos de Concepción, San Pedro y Amambay.

Así mismo, con el establecimiento del Comando de Operaciones de Defensa Interna (CODI), con los elementos mejor preparados y con la mayor capacidad operacional de la fuerza, puede convertirse en una herramienta de apoyo principal en ciberdefensa y ciberseguridad en su área de responsabilidad en función a la Política de Ciberdefensa contribuyente a la Política de Defensa Nacional 2019 – 2030 del Paraguay.

Se cumplieron con el objetivo general de la investigacion analizando la importancia de ciberdefensa y ciberseguridad para la proteccion del ciberespacio en el marco de las operaciones militares que realiza el Comando de Operaciones de Defensa Interna (CODI), a traves de los tres objetivos especificos.

En el capitulo uno, se desarrollo las diversas ciberamenazas que pueden afectar una operación militar y en especial las acciones realizadas por el Comando de Operaciones de Defensa Interna (CODI), estas amenazas tambien puede ser provenido de actores malintencionados, como grupos ciberdelincuentes, hackers, espías cibernéticos o incluso de agencias gubernamentales hostiles.

Estos ataques pueden paralizar las comunicaciones y los sistemas de mando y control, dificultando la coordinación y la toma de decisiones en una operación militar. Los programas maliciosos, como virus, gusanos y troyanos, pueden infectar sistemas y redes militares, permitir a los atacantes robar información confidencial, alterar datos o controlar los sistemas de manera remota. Esto puede dañar la estructura y la seguridad de las operaciones militares.

Este tipo de ataques involucra manipular a individuos para obtener información confidencial o acceder a sistemas. Los atacantes pueden utilizar técnicas como la suplantación de identidad, el phishing o el engaño para obtener credenciales de acceso o información sensible.

Los grupos armados al margen de la ley y demas grupos delictivos, que operan en la zona norte de Paraguay pueden utilizar tácticas de desinformación en línea para difundir información falsa o engañosa con el fin de influir en las operaciones militares. Es importante tener en cuenta que estas amenazas pueden evolucionar rápidamente, y los adversarios cibernéticos están constantemente buscando nuevas formas de explosión de vulnerabilidad. Por lo tanto, la ciberseguridad y la ciberdefensa deben ser dinámicas y adaptarse a las amenazas emergentes para garantizar la seguridad de las operaciones militares.

En el capitulo dos, se desarrollo la ciberseguridad más adecuada para ser empleada en operaciones militares, que debe tener en cuenta la naturaleza específica de las operaciones y los requisitos de seguridad de las fuerzas armadas. Algunos aspectos clave de ciberseguridad que son especialmente relevantes en este contexto incluyen; una estrategia de defensa en profundidad que implica utilizar múltiples capas de seguridad para proteger los sistemas y las redes.

Dado que las comunicaciones son esenciales en las operaciones militares, es importante garantizar la seguridad de las redes y los sistemas de comunicación utilizados. Esto implica utilizar protocolos de cifrado fuertes para proteger la confidencialidad de la información

transmitida y autenticación robusta para garantizar la identidad de los participantes en la comunicación. La protección de infraestructuras críticas militares, como sistemas de comando y control, sistemas de armas y centros de datos, deben ser especialmente protegidos mediante medidas de seguridad física, como sistemas de vigilancia y acceso restringido, así como medidas de seguridad lógicas, como sistemas de detección de intrusos y redundancia de datos.

A pesar de los esfuerzos de prevención, es posible que se produzcan incidentes de seguridad. Por lo tanto, es esencial contar con planes de contingencia y estrategias de recuperación para minimizar el impacto y restaurar rápidamente las operaciones normales después de un incidente. Esto puede incluir sistemas de copia de seguridad y restauración, así como la capacidad de análisis forense para investigar las causas del incidente.

La ciberseguridad más adecuada para ser empleada en las operaciones militares debe ser integral, incluyendo técnicas organizativas, y adaptar a los requisitos específicos de seguridad de las fuerzas armadas. La defensa en profundidad, la seguridad de las comunicaciones, la protección de infraestructuras críticas, la vigilancia y detección temprana, la resiliencia y recuperación, así como la formación y concienciación del personal.

En el capitulo tres, se desarrollo una investigacion sobre el personal y los equipos especiales de ciberseguridad y ciberdefensa que podrian ser propuesto al Comando de Operaciones de Defensa Interna (CODI), quienes y que desempeñan un papel crucial en la protección de las redes, sistemas e información contra amenazas cibernéticas. El personal debera tener experiencia en la implementación de medidas de seguridad cibernética, como firewalls, sistemas de detección de intrusiones, autenticación multifactor y cifrado de datos, porque seran responsables de monitorear la infraestructura cibernética en busca de posibles vulnerabilidades y responder a incidentes de seguridad.

El personal especialistas recopilaran y analizaran información de inteligencia relacionadas con ciberamenazas y ataques cibernéticos, utilizando técnicas de análisis para

identificar patrones y tendencias en el comportamiento de los adversarios cibernéticos y proporcionaran información valiosa para la toma de decisiones al comandante para la realizacion de las operaciones militares.

Los equipos especiales estáran preparados para responder rápidamente a incidentes de seguridad cibernética, cuyo objetivo sera identificar y contener la amenaza, recuperar los sistemas afectados y llevar a cabo un análisis forense para determinar la causa del incidente.

En algunas operaciones militares, puede haber equipos especializados en ciberoperaciones ofensivas para identificar y explotar las vulnerabilidades en las redes y sistemas enemigos, con el fin de obtener inteligencia o debilitar las capacidades del adversario.

Además de los equipos especializados, el Comando de Operaciones de Defensa Interna (CODI), debera contar con personal capacitado en prácticas seguras de manejo de la información y en la identificación de posibles amenazas cibernéticas. La ciberseguridad es una responsabilidad, y el entrenamiento y concienciación del personal son fundamentales para prevenir incidentes de seguridad compartidos.

Es importante que estos equipos trabajen en colaboración con otros especialistas en inteligencia, operaciones militares y seguridad física para asegurar una defensa integral y efectiva en el entorno cibernético. Además, deben mantenerse actualizados con las últimas tendencias y desarrollos en el campo de la ciberseguridad para estar preparados para enfrentar amenazas emergentes y destacadas.

Proyectar, las capacidades de la institución a través de la aplicación eficaz de acciones de ciberseguridad y el soporte a acciones de ciberdefensa, centralizando esfuerzos para incrementar las condiciones de seguridad del ciberespacio en su área de responsabilidad.

Con el desarrollo del objetivo general de la investigacion, se considera necesario la creación de un destacamento de ciberdefensa para operaciones militares realizadas por el

Comando de Operaciones de Defensa Interna (CODI), que requieran coordinación tanto a nivel estrategico, operacional y táctico.

Además, es necesario mencionar que en el área de responsabilidad territorial del Comando de Operaciones de Defensa Interna (CODI), existen infraestructuras críticas de instituciones del estado que afectadas crearia un caos poblacional, que por tal motivo también deben ser objeto de atención por lo sensible que puede representar las mismas, el Comando de Operaciones de Defensa Interna, tiene lo genéricamente necesario para ir intensificando las operaciones militares de ciberdefensa y ciberseguridad, es necesario enfatizar estos aspectos por la importancia de su área de responsabilidad y la mision.

Además, esta investigación es un recurso que sirve de guía para la protección del ciberespacio en apoyo de las operaciones militares; en particular, tienen la visión de cómo operar con las nuevas capacidades y estrategias que se adopten, proporcionando el salto necesario que deberá ser consolidada a futuro en un proyecto de modernización que establezca capacidades para una optimización de la institución.

Finalmente, al haber dado cumplimiento a los objetivos específicos mencionados también se da cumplimiento al objetivo general al haber analizado la importancia del empleo de la ciberdefensa y la ciberseguridad en las operaciones militares del Comando de Operaciones de Defensa Interna (CODI), para la protección del ciberespacio.

Considerando, todo lo mencionado en los párrafos anteriores, se presenta a continuación una propuesta para la creación de un destacamento de ciberseguridad con un plan para implementar efectivamente y fijar acciones de apoyo.

PROPUESTA PARA EL COMANDO DE OPERACIONES DE DEFENSA INTERNA (CODI)

La creación del destacamento de ciberdefensa para las operaciones militares dentro del entorno del ciberespacio, de acuerdo a las misiones encomendada via decreto presidencial y la modicacion de la ley de Defensa Nacional para el Comando de Operaciones de Defensa Interna (CODI), que requieran de una mayor coordinación a nivel estrategico, operacional y táctico entre la Fuerza de Tarea Conjunta (FTC), Batallon de Inteligencia Militar (BIMI), Equipos Tacticos de la Policia Nacional (PN) y la Secretaria Nacional Antidrogas (SENAD), todas estas instituciones son componentes del Comando de Operaciones de Defensa Interna (CODI), creada para la pacificacion de la zona norte de la Republica del Paraguay.

Las posibilidades y limitaciones de la estructura del destacamento responsable de guíar las acciones de ciberdefensa y ciberseguridad de las operaciones militares necesariamente debe estar directamente subordinado al Comando Operaciones de Defensa Interna (CODI), como una sub unidad a cargo de un Oficial Superior con curso de Estado Mayor experto en ciberdefensa y ciberseguridad.

Los detalles de conformacion de la estructura y el personal deben definirse después de un estudio e informe del Estado Mayor General del Comando de Operaciones de Defensa Interna (CODI), y propuesto al comandante, quien deberá decidir de acuerdo a los factores de la decisión y la mision de la institucion.

Es deseable que, en el diseño de la estructura, haya una separación en cuanto a la planificación y ejecución de las acciones para proteger a las personas de la explotación y el ciberataque.

Entre los muchos aspectos tratados, se debe trabajar en la elaboración de un programa de ciberdefensa y ciberseguridad como objetivo principal, diseñar de modo integral y consensuado, doctrinas y procedimientos a ser normados y aplicados por el Comando de

Operaciones de Defensa Interna (CODI), acorde a los estándares establecidas de acuerdo al Plan Nacional de Ciberseguridad.

La aplicación del programa permitirá la prevención, detección y mitigación de los ataques cibernéticos, como así también, la investigación y el diseño de nuevas estrategias específicas para cada área de las unidades que dependan organizacional y administrativamentente en las operaciones militares del Comando de Operaciones de Defensa Interna (CODI).

Incorporar, capacitar y gestionar los recursos humanos necesarios, incluyendo a los propios militares que operan en la zona norte dentro de la organización del Comando de Operaciones de Defensa Interna (CODI), definir y actualizar los perfiles del personal necesario para definir mecanismos de retención del personal militar y si es necesario incorporar personal civil especialistas con experiencia y conocimientos.

Capacitar al personal en forma continua para mantener su competencia profesional, como aquellos provenientes del medio civil; promover becas de estudios y especialización en otras organizaciones y en el extranjero dependiendo del presupuesto que pueda conseguir el comandante. Elaborar y aplicar normas de estandarización según necesidades de desarrollo y diseño del destacamento de ciberdefensa.

Promover el desarrollo y empleo de sistemas que empleen redes y medios de comunicación de uso militar exclusivo, proponer la elaboración de una doctrina de ciberdefensa para el Comando de Operaciones de Defensa Interna (CODI), y desarrollar programas de capacitación y concientización para los miembros de la institucion.

Establecer la estructura con los estándares desarrollados y publicados por la Organización Internacional de Normalización (ISO) 27001 como referencia especializada para la normalización a nivel mundial sobre ámbitos tales como la seguridad de la Información.

Posibilidades del destacamento de ciberdefensa

El aprovechamiento del éxito consiste en aprovechar, retener y explotar la iniciativa y beneficiarse de la disminución, ya lograda, de la capacidad de ciberdefensa del adversario, anulando o desequilibrando sus posibilidades de acción o reacción para;

1) Identificar y analizar vulnerabilidades (conocidas) en las redes y aplicaciones informáticas utilizadas en el sistema de comando y control implementado para las operaciones militares.
2) Recomendar acciones para mitigar las vulnerabilidades identificadas.
3) Estudiar las amenazas y comprender su impacto en las redes de comando y control o cualquier otra estructura y/o recursos humanos.
4) Verificar el cumplimiento de la seguridad de la información y las comunicaciones en el sistema de comando y control implementado para las operaciones militares.
5) Asesorar al comandante del Comando de Operaciones de Defensa Interna (CODI), a los de efectos deseados por el escalón superior.
6) Colaborar con la ejecución de la información operativa planificada; y colaborar con el esfuerzo de obtener datos para la producción de conocimiento de inteligencia, a través de la fuente cibernética, en el contexto de las operaciones militares de conformidad con las directrices y directivas emitidas por las Fuerzas Militares (FF.MM.)

Referencias

O'KUINGHTTONS, Ú. (16 de mayo de 2017). *EL PAIS* . Obtenido de https://elpais.com/tecnologia/2017/05/13/actualidad/1494680920_206684.html

Caceres, C. J. (2019). *La capacidad de respuesta a las amenazas a la Ciberdefensa y Ciberseguridad en el ambito de las Fuerzas Militares.* Asuncion: IAEE.

Ciberdefensa, P. d. (2021). *Resolucion 573.* Asuncion: Ministerio de Defensa Nacional.

Vergara, G. D.-C. (2016). Operaciones Militares Ciberneticas. Cuidad Autonoma de Buenos Aires, Capital Federal.

CERT-PY. (2020). *Ciberseguridad Paraguay 2020.* Asuncion: MITIC.

Locatelli, O. A. (2017). Guerras híbridas su centro de gravedad y la victoria. *CEFA DIGITAL*, 41-42.

Bartolome, M. C. (s.f.). *teseopress.com*. Obtenido de https://www.teseopress.com/contrapuntos/chapter/13-la-ciberseguridad-en-el-siglo-xxi-y-la-situacion-de-america-latinafootnote-el-presente-capitulo-de-libro-constituye-una-extension-del-trabajo-titulado-las-ciberamenazas-y-su-impacto-en/

Ganuza, N. (2020). *Ciberdefensa.* Canada: IADF.

Cano, M. E. (2018). *Amenazas Cibernéticas a la Seguridad y Defensa Nacional.* Colombia: urosario.

MITIC. (25 de Abril de 2017). *Plan nacional de ciberseguridad.* Asuncion: Mitic.

Baretto, J. F. (2017). *LA DEFENSA NACIONAL Y LA ESTRATEGIA MILITAR DE SEGURIDAD CIBERNÉTICA.* CABA.

Duran, J. j. (2011). *La Ciberseguridad en el ambito militar.* España.

Antonio, J. M. (2021). *Ciberamenzas a la seguridad nacional y politica exterior.* Chile: Instituto de Estudios Internacionales.

Flores, F. S. (2021). *La adaptación asimétrica de las doctrinas de Defensa en torno al ciberespacio: los casos de Chile y Ecuador (2014 -2018)* . Quito - Ecuador: Facultad Latinoamericana de Ciencias Sociales, FLACSO Ecuador .

Miranda., C. d. (2016). *ESPECIALIZACIÓN EN ESTRATEGIA OPERACIONAL Y PLANEAMIENTO MILITAR CONJUNTO.* Cuidad Autonoma de Buenos Aires: Escuela Superior de Guerra Conjunta.

BARROS, M. L. (2022). LASOPERACIONESDE CIBERDEFENSA-ESTUDIO DECASOSENARGENTINA YBRASIL. *RESGA*, 38.

Ortega, L. F. (2012). *La ciberdefensa y ciberseguridad.* Imprenta Ministerio de Defensa Nacional de España.

Martin, C. (5 de septiembre de 2022). *GlobalSuite Solutions*. Obtenido de Google: https://www.globalsuitesolutions.com/es/normas-iso-para-mejorar-la-ciberseguridad/

Caro Bejarano, M. J. (2011). *ALCANCE Y ÁMBITO DE LA SEGURIDAD NACIONAL EN EL CIBERESPACIO.* Dialnet.

Vargas, E. M. (2014). *CIBERSEGURIDAD Y CIBERDEFENSA.* BOGOTÁ D.C.: UNIVERSIDAD MILITAR NUEVA GRANADA.

Cabrera, M. C. (2019). *Empleo de las redes informáticas en Ciberoperaciones en el marco de la Gran Unidad de Batalla.* Ciudad Autónoma de Buenos Aires.

ANEXO 01 – ENTREVISTA

AL EX COMANDANTE DEL BATALLON DE INTELIGENCIA MILITAR (BIMI)

Grado, Nombre y Apellido: Cnel DCEM Adolfo Fernández Encina

Puesto o cargo que ocupa: Sub Director General de la Dirección de Material Bélico (DIMABEL)

Tiempo en el cargo: Año 2019 hasta la actualidad

1. **Cuál es la situación actual de ciberdefensa y ciberseguridad en Paraguay.**

Podría considerarse en una etapa de maduración temprana, afianzándose de manera progresiva, sin embargo, para que las Fuerzas Militares puedan cumplir su misión de proteger al Estado, particularmente en el ámbito de ciberdefensa y ciberseguridad se debe tener la capacidad de proteger la infraestructura critica propia y de todo el Estado.

El personal que conforma actualmente la DIGETIC, pionera en la gestión y aplicación de la ciberdefensa en el país, se encuentra con falta de equipamientos y que podría ser considerado fundamental al momento de la conformación de un Destacamento Conjunto de Ciberdefensa teniendo en cuenta que el personal capacitado es un factor importante para su funcionamiento.

La ciberdefensa debe ser fortalecida y lograr un nivel de maduración, tal que podamos realmente defendernos de posibles ataques cibernéticos de gran impacto y proteger las infraestructuras críticas.

2. **¿Cuáles son las ciberamenazas dentro de las operaciones militares que pueda afectar el ciberespacio?**

El Comando de Operaciones de Defensa Interna, por lo sensible de sus operaciones y contar con la mejor infraestructura criticas operativa de las fuerzas armadas en tecnología de inteligencia y comunicaciones, debe estar en el interés de varios grupos delictivos.

Para tal efecto tiene la imperiosa necesidad de proteger sus sistemas informáticos y de intensificar sus políticas de seguridad de la información.

3. **¿Cómo son abordados el empleo de la ciberdefensa y ciberseguridad en las operaciones militares?**

Considero que actualmente la ciberdefensa y ciberseguridad no es abordada como prioridad de forma efectiva en las operaciones militares y tampoco tienen herramientas actuales para aplicar una política de seguridad de la información y protección de datos.

4. **¿Cuáles son las acciones aplicables al empleo de ciberdefensa y ciberseguridad a las operaciones militares?**

Asegurar el empleo de la TIC de manera eficiente, protegiendo los activos de gestión de información, capacitación, concienciación sobre las amenazas que existen en el ciberespacio y establecer un protocolo de seguridad con manual de proceso interno para evitar la fuga de información.

5. **¿Cuál es la importancia del empleo de ciberdefensa y ciberseguridad en las operaciones militares para la protección del ciberespacio?**

Es fundamental el empleo, ya que se maneja varias informaciones sensibles, y bien se sabe que uno de los principios que manejamos como personal militar es la seguridad, su importancia implica en la protección contra ataques de personas inescrupulosas que deseen acceder para dañar o perjudicar las acciones de las operaciones militares.

6. **¿En su área de responsabilidad cuenta con infraestructuras críticas y cuáles son de forma genérica?**

Si se cuenta, sub estática de la ANDE, los tendidos de alta tensión, los locales de las gobernaciones y de las municipalidades, Palacio de Justicia, todos interconectados a la red, sistema de comunicaciones y sistemas de gestión de información.

ANEXO 02 – NIVELES DE ALERTAS AMENAZAS PARAGUAY

AMENAZAS			
Color	**Identificación**	**Descripción**	
Gris	Bajo	No afectan el Ciberespacio.	Normal funcionamiento de las actividades.
Verde	**Moderado**	Afectan el Ciberespacio, sin comprometer las Infraestructuras Críticas de la Información.	Posibilidad de ejecución de las amenazas.
Azul	**Mediano**	Acciones cibernéticas escalan afectando el Ciberespacio, sin comprometer las Infraestructuras Criticas.	Aplicable cuando la percepción de la amenaza con la Infraestructura Critica.
Naranja	**Alto**	Acciones cibernéticas hostiles afectan parcialmente las Infraestructuras Criticas.	La Infraestructura Crítica fue vulnerada, pera tiene la capacidad de resiliencia.
Rojo	**Muy alto**	Acciones cibernéticas hostiles, exploran o niegan la disponibilidad de la Infraestructura Critica de la Información.	La Infraestructura Crítica fue vulnerada y va a tardar en recuperarse.

Fuente: digetic.ffmm,mil,py

ANEXO 03 – ESQUEMA GRÁFICO METODOLÓGICO