Facultad del Ejército
Escuela Superior de Guerra
"TG Luis María Campos"

TRABAJO FINAL INTEGRADOR

Título: "La seguridad del Sistema de Comunicaciones e Informática Particular, ante las amenazas de la Ciberguerra y Guerra Electrónica".

Que para acceder al título de Especialista en Conducción Superior de OOMMTT, presenta el Mayor PERALTA Santiago

Director de TFI: TC Juan Carlos GUERRA

Ciudad Autónoma de Buenos Aires, 04 de abril de 2024.

Resumen

Un comandante del Componente Terrestre podrá comandar y controlar las operaciones mediante el establecimiento de un Sistema de comunicaciones e informática particular (SCIP), el cual se ha convertido en una pieza importante dentro del centro de gravedad del dispositivo.

El presente trabajo busca determinar las vulnerabilidades críticas que posee un SCIP, las cuales serán objeto de ataque, por medio de diferentes acciones que ejecutara el enemigo a través de la ciberguerra y la guerra electrónica.

La presente investigación permitirá arribar a conclusiones finales, donde se procederá a reunir y organizar toda la información obtenida, para poder identificar las acciones a adoptar con el fin de asegurar y proteger los propios medios de las operaciones del adversario, a fin de permitir un ágil, seguro y confiable sistema de comando y control, que asegura la conducción de las operaciones del nivel Componente Terrestre.

Palabras claves: Comando y control, Comunicaciones e Informática, Centro de gravedad, Ciberguerra, Guerra electrónica.

Índice

Índice de Tablas

Índice de Figuras

Introducción

Presentación del Problema

Actualmente los sistemas de comunicaciones e informáticos se han convertido en una herramienta fundamental en un teatro de operaciones, permitiendo acceder a una amplia gama de servicios y comunicarnos en forma instantánea y eficiente. Sin embargo, esta gran dependencia de la tecnología también implica un mayor riesgo de amenazas y ataques, colocando al sistema como el centro de gravedad de las acciones ofensivas del enemigo.

En este contexto, la guerra electrónica y los ciberataques se han vuelto una preocupación creciente. Estas actividades buscan perturbar, dañar o acceder de manera ilegal a los sistemas de comunicación e informáticos, con el fin de obtener información confidencial, manipular datos o interrumpir servicios esenciales necesarios para la conducción de las operaciones y para el proceso toma de decisiones.

La presente investigación apunta a la identificación de las vulnerabilidades críticas, centrando el estudio en la comparación de estas con las amenazas planteadas por los ataques del adversario, con la finalidad de poder obtener conclusiones que permitan tomar las medidas necesarias para proteger y fortalecer la seguridad de estos sistemas, y garantizar su correcto funcionamiento.

En función de lo expresado y a los efectos de definir los límites y el alcance de la investigación, la misma se define por el interrogante de ¿Cuáles son las vulnerabilidades críticas del SCIP a ser afectadas por las acciones de ciberguerra y GE del enemigo?

Fundamentos y Motivación para la Investigación

Los conflictos bélicos más actuales y recientes, han dejado muy en claro la importancia decisiva de las comunicaciones para permitir la coordinación y control de las diferentes operaciones militares ejecutadas dentro de un teatro de operaciones.

En las operaciones, participan un número variado de elementos que se combinan en diferentes sistemas de armas, los mismos interactúan entre sí en forma coordinada y sincronizada, bajo el concepto sistémico. Por tal motivo en gran medida el éxito de la operación dependerá de un sistema de comunicaciones e informática que facilite el comando y control de la fuerza en pleno ejercicio de las actividades básicas de la conducción.

> Un sistema de comando, control, comunicaciones, informática e inteligencia (C^3I^2), es un conjunto de medios humanos, equipos y materiales de alta tecnología que integrados y estructurados en forma automatizada y por medio de procedimientos normalizados, posibilitara al comandante y a su órgano de asesoramiento, ordenar, controlar, comunicase, conocer la situación de otras fuerzas amigas, las condiciones del terreno, las condiciones meteorológicas y al enemigo y sus acciones, cuasi en tiempo real. (Ejército Argentino, 2016, págs. Cap I - 5)

El sistema de comunicaciones e informática particular (SCIP), no es simplemente una herramienta para poder recibir o transmitir un mensaje, todo lo contrario, debe cumplir con requisitos fundamentales tanto en la paz como en la guerra; “ellos son confianza, seguridad y rapidez”. (Vicenti., 2014, pág. 4)

Teniendo en cuenta los requisitos mencionados anteriormente, hay que tener presente que no se debe sacrificar o comprometer uno de ellos en beneficio de otros, ya que el sistema de comunicaciones quedaría expuesto a las acciones del enemigo, comprometiendo el éxito de la operación.

En las últimas décadas del siglo XX, podemos identificar en el campo de combate, el empleo intensificado de nuevas tecnologías de comunicaciones, como los complejos sistema de encriptados, salto de frecuencia, nuevas formas de ondas y de modulación, troncalizadores, medios satelitales y de telefonía.

La incorporación de la informática, la cual produjo una evolución tecnológica en el ámbito de las comunicaciones, que se fue manifestando de manera constante y muy rápida, ha provocado la implementación de nuevos equipos, técnicas y conocimientos necesarios por parte del personal, sobre el uso de redes y conectividad digitales e informatización de los equipos. Provocando la incorporación de equipos de comunicaciones y dispositivos informáticos idóneos a los avances tecnológicos de la actualidad.

Las nuevas Tecnologías de la Información y Comunicación (TICs) han llevado al mundo a una interconexión instantánea, permitiendo observar los conflictos armados suscitados en diferentes países, los ciberataques de manera online y el manejo de la información en los conflictos actuales.

La utilización de las TICs, en los conflictos armados tiene su origen de la Segunda Guerra Mundial, donde se desarrollaron diferentes diseños y fabricaciones de nuevas armas de larga distancia, a su vez se mejoraron los sistemas de reconocimiento de imágenes, detección de objetivos y sistemas electromagnéticos.

> La revolución tecnológica que se observa en el último siglo no sólo logra una modificación del funcionamiento del instrumento militar y propagandístico, sino que además conlleva una revisión y actualización de la doctrina y el modelo de organización tradicional de los ejércitos, obligando a tener que adaptarse a la tecnología y plasmar una nueva visión global de tácticas y estrategias militares basadas en el conocimiento que se posea sobre las TICs. (Caballero, 2003)

El avance en la tecnología ha llevado a la Fuerza a emprender un proceso de reconversión, el cual requiere de una restructuración del apoyo de comunicaciones e informática previsto. Es así que el Componente terrestre debe disponer de una estructura fija y de campaña confiable, segura y ágil, que posibilite a los Comandos, Organismos y Elementos

que la componen, establecer un C^3I^2 para el desarrollo de las operaciones tácticas y las operaciones subsidiarias en las que participen las fuerzas terrestres.

Con relación al ámbito de las comunicaciones, se requieren un elevado nivel de integración entre las facilidades de comunicaciones e informática, permitiendo a un Centro de Comunicaciones Informático (CCI) brindar todos los servicios necesarios de voz y datos a un comandante, para que el mismo pueda ejercer su comando y control en forma eficiente sobre la Fuerza que conduce.

En los últimos años, hubo un incremento notable en materia de inversión, en lo que respecta a la incorporación de material tecnológicos a través del Ministerio de Defensa, pudiendo citar:

- Telepuerto Satelital del Ejército Argentino: Es la estación donde se concentra las señales satelitales de alta capacidad de la Fuerza. Esta capacidad permite la gestión propia de los enlaces satelitales, independizándonos de contratos y proveedores privados.
- Terminal Satelital de Campaña Remolcable (TSCR): Consiste en estaciones satelitales transportables robustas para uso en el terreno. Representa el punto de acceso de banda ancha más importante de las tropas en campaña, incrementando notablemente el nivel de comando y control de la Fuerza.
- Centro de Comunicaciones Móvil Integrado (CCMI): Se trata de una moderna facilidad móvil que permite la integración de servicios de voz y datos para el apoyo de centros de comunicaciones en el terreno, constituyendo parte de los Centros de Comunicaciones y Puestos Comando de Brigadas (GUC) y Divisiones de Ejército (DE).
- Centro Troncalizador de Comunicaciones Móvil (CTCM): Permiten satisfacer los requerimientos de comunicaciones en tareas de apoyo a la comunidad y

operacionales propias del Ejército. Los CTCM brindan acceso satelital a la red estratégica y de distribución local de la información integrados en un único vehículo/shelter, autosuficiente en cuanto al traslado del personal y a las necesidades energéticas para funcionar en forma autónoma.

- Centro Troncalizador de Video Móvil (CTVM): Complementando los requerimientos de Comando y Control del campo de combate moderno, se desarrollaron sistemas de transmisión de video de alta definición (HD) desplegables en el terreno, para la transmisión de video y videoconferencia en campaña, en tiempo real, por vínculo satelital o cualquier otro medio de alta capacidad de datos instalado en el terreno.
- Radioenlaces Digitales de Campaña (RDC): Las necesidades de acceso y distribución de información en operaciones o en zonas de emergencias demandan de sistemas terrestres inalámbricos de banda ancha para cumplir con este requerimiento, estos potentes sistemas de campaña de alta capacidad, con alcance efectivo a distancias de hasta 40 Km.
- En lo referente a equipamiento radioeléctrico táctico, se cuenta con equipos militares de última generación, que permiten las comunicaciones de voz y datos seguras (encriptado y salto de frecuencia), con normas de robustez ambientales acordes al uso militar (Normas STD MIL), en las bandas de HF, VHF y UHF.

Lo mencionado hasta el momento, evidencia como los sistemas actuales de comando y control, están compuestos por componentes electrónicos avanzados, que incluyen software embebido en ellos. La evolución tecnológica hace necesario el uso del ciberespacio, ganando capacidades, pero a la vez exponiendo vulnerabilidades críticas.

Las vulnerabilidades de nuestros sistemas, una vez que hayan sido identificadas por el enemigo, serán afectadas por dos acciones que hay que debemos identificar, la Ciberguerra y

la Guerra Electrónica. No hay que confundirlas, ya que los ámbitos de aplicación son diferentes: el primero se da en el dominio electromagnético, y el segundo en el ciberespacio.

La ciberguerra, incluye acciones defensivas, para proteger del enemigo los sistemas de información y acciones ofensivas, para negar / neutralizar su uso por parte del enemigo, y constituye una importante fuente de información de inteligencia. Desarrolla acciones que se pueden percibir en forma directa, por sus resultados, como la negación de un servicio, pero también otras imperceptibles, muy peligrosas, con consecuencias variadas.

La guerra electrónica (GE) se desarrolla en el dominio electromagnética, el cual es crucial en la guerra moderna, puesto que por él se comunican y comandan las fuerzas del Componente Terrestre (Comando y Control). Los sensores pueden detectar amenazas a tiempo, y se pueden guiar sistemas de apoyo de fuego, para citar algunos ejemplos. Incluye acciones defensivas, para asegurar el uso propio del espectro electromagnético por parte de la propia fuerza, y acciones ofensivas, tendientes a obtener información y negar al enemigo el uso de su espacio electromagnético, con lo cual afecta el comando y control.

Los antecedentes mencionados anteriormente, sumado a las acciones que se pudieron observar al inicio del conflicto entre Rusia y Ucrania, nos muestra como el centro de gravedad se focalizó en los puestos comando y su SCIP, con el fin de afectar el comando y control de las operaciones en curso.

“Las potencias de primer orden ya han sufrido acciones que mostraron sus vulnerabilidades, lo comprendieron y han alineado sus estrategias de recursos – modos y fines” (Zarza, 2016, pág. 7), para asegurar principalmente el sistema C^3I^2, de las acciones de GE y ciberguerra del enemigo.

En función de lo citado anteriormente, esta investigación pretende analizar el sistema de comando y control, materializado por SCIP que brinda apoyo al Componente Terrestre, para

identificar las vulnerabilidades críticas que presenta y poder adoptar las acciones correctivas con el fin de proteger a la Fuerza de potenciales acciones del enemigo. Permitiendo que nuestro sistema de defensa posea los medios y capacidades adecuadas para ejercer un monitoreo aeroespacial y del ciberespacio y así brindar las alertas pertinentes que permitan accionar en tiempo y espacio, con el objetivo de asegurar nuestro centro de gravedad.

Objetivo de la Investigación de Estado Mayor

Objetivo General

Identificar las vulnerabilidades críticas del SCIP a ser afectadas por las acciones de ciberguerra y GE del enemigo, para determinar las acciones a adoptar, con el fin de asegurar un ágil, seguro y confiable sistema de comando y control.

Objetivo Específico Uno

Analizar y observar los procesos de trabajo ejecutados dentro de un centro de comunicaciones informático en apoyo a un puesto comando, para determinar las vulnerabilidades críticas que serán afectadas por el enemigo.

Objetivo Específico Dos

Comparar y evaluar las vulnerabilidades críticas con las acciones de ciberguerra y guerra electrónica, para determinar el nivel de riesgo del sistema de comando y control.

Objetivo Específico Tres

Analizar y evaluar la seguridad de un SCIP, para identificar las acciones a corregir, con el propósito de asegurar nuestras vulnerabilidades y permitir un adecuado comando y control de las operaciones.

Explicación del Método:

El método a emplear será el deductivo.

Diseño de la Investigación:

El diseño de la investigación será de tipo explicativo.

Técnicas de Validación:

Análisis bibliográfico, documental y lógico.

Capítulo I

Sistema de Comunicaciones e Informático Particular

El presente capítulo se desarrollará con la finalidad de analizar y observar los procesos de trabajo de un Centros de Comunicaciones e Informática Particular en apoyo a un puesto comando de Componente Terrestre. Para lograr el mencionado propósito, se definirá doctrinariamente el concepto, se lo describirá a través de su clasificación, organización, composición, funciones; y se analizarán los roles de los integrantes y misiones particulares de cada personal. Además, se definirá un concepto de centro de gravedad y se indicarán las vulnerabilidades críticas que presenta el SCIP.

Sección I

Centro Comunicaciones e Informático Particular

Conceptos Generales

Antes de desarrollar el SCIP, es preciso definirlo, y luego establecer la relación entre éste y el comando y control.

Las telecomunicaciones es un concepto que abarca las comunicaciones y la informática, hay varias definiciones desarrolladas que podemos encontrar de diversos autores, pero la adoptada y empleada en él (Ejército Argentino, 2016) es, “todos los modos de transmitir información a distancias a través de las diferentes facilidades y medios, incluidos los informáticos que sirvan con la finalidad de emitir, transportar y recibir entre dos o más puntos”. (págs. Cap I – 2)

Referido a la informática, en la actualidad adquiere una relevancia sumamente importante en las operaciones militares, debido que contribuye al comando y control, tanto en la etapa de planeamiento y ejecución de las acciones.

Cuando nos referimos a un SCIP en apoyo a un elemento, independientemente del nivel o magnitud que se trate, debemos entender al sistema como un "conjunto de medios e instalaciones de comunicaciones e informática que son instaladas, operadas y mantenidas, con la finalidad de contribuir al comando y control de la Fuerza durante el desarrollo de una operación militar" (Ejército Argentino, 2016).

Dentro de las principales facilidades y medios que serán utilizados para brindar el apoyo necesario, podemos mencionar:

- Cableadas o guiadas: están conformadas principalmente por cable de campaña, UTP, cable multipar, fibra óptica, etc. Esta facilidad se utiliza para interconectar a diferentes usuarios dentro de un mismo o distinto comando, unidad, subunidad independiente y a otros organismos de la fuerza, permitiendo el intercambio de un elevado volumen de información a través de distintas terminales.
- Radioeléctricas: en campaña, estará conformado por los diversos enlaces entre los puestos radioeléctricos en apoyo a los comandos, elementos y organismos de la fuerza, permitiendo el comando y control de una operación táctica o una subsidiaria.
- Radioenlaces digitales: permite la transmisión de información en voz, datos, imágenes y video entre dos terminales y posibilitando la integración del sistema de campaña con las facilidades de REDISE desde un Centro de Comunicaciones e Informático Guarnicional (CCIG) o desde un punto de acceso a los sistemas comunicaciones territoriales
- Satelitales: proporciona facilidades de comunicaciones en voz y datos, integrando a los sistemas de campaña con la REDISE. Es un medio de gran movilidad y fácil de transportar, apto para brindar apoyo en todo tiempo y lugar, principalmente al comando y control de las grandes unidades.

- Estafetas: personal instruido y adiestrado para la transmitir y recibir mensajes por medio físico dentro de un puesto comando y centro de comunicaciones. También podrán ser empleados entre diferentes elementos, debido a la seguridad que proporcionan en el diligenciamiento del mensaje.
- Sónicas: “son aquellas ondas sonoras que se transmiten por medio de silbatos, cornetas, sirenas y otros instrumentos para enviar señales de advertencia o atención. Normalmente, serán utilizadas para la transmisión de mensajes cortos y sencillos, previamente convenidos y para difundir alarmas”. (Ejército Argentino, 2016, págs. Cap I - 20)
- Visuales: transmisión de mensajes breves a distancias cortas y para el reconocimiento de fuerzas amigas, los cuales son recibidos a simple vista o por medio de la utilización de medios ópticos.

Sistema de Comando, Control, Comunicaciones, Informática e Inteligencia

El Sistema de comando y control empleado en el Ejército, ha atravesado a lo largo de su historia variadas modificaciones, pasando desde C3I -comando, control, comunicaciones e inteligencia-, C2TI -comando, control, teleinformática e inteligencia-, llegando hasta su denominación actual C3I2, el cual ya fue conceptualizado en oportunidad.

Éste está integrado por una serie de Subsistemas:

a) Subsistema de comando: Compuesto por el personal integrante del Puesto Comando: comandante/jefe, su/s estado mayor/es, auxiliares y operadores.
b) Subsistema de control: Integrado por el personal mencionado en el punto anterior, sumado los conjuntos de sensores, procedimientos y mecanismos de empleo de estos.

c) Subsistema de inteligencia: Integrado por el personal y tropa técnica de inteligencia.

d) Subsistema de comunicaciones e Informática: es la columna vertebral del sistema de comando y control, se compone por el personal de comunicaciones y del sistema de cómputo de datos.

Las características funcionales y operativas que debe reunir un sistema C^3I^2, diseñado para brindar apoyo a un Comando del nivel componente terrestre, son las siguientes:

a) Confiable, en cuanto el sistema debe garantizar el ejercicio del comando ininterrumpidamente, logrando la confiabilidad del sistema mediante la redundancia de las facilidades instaladas.

b) Ata capacidad de supervivencia: característica fundaméntela para poder hacer frente a las acciones de GE, ciberataques, ataques desde la superficie y desde el espacio aéreo y poseer la capacidad de evasión y engaño para evitar ser localizado.

c) Amigable para el usuario: mediante el establecimiento de procedimientos sencillos, familiares e intuitivos para el operador.

d) Seguro: contar con las herramientas necesarias para procesar la información y al mismo tiempo negarla al enemigo y personal no autorizado.

e) Potente: en cuanto al proceso de obtención y procesamiento de datos, facilitando de esta forma el planeamiento.

f) Flexible: ser capaz de adaptarse ante cualquier cambio de situación.

g) Móvil: deberá poseer el mismo grado de movilidad que el elemento apoyado.

h) Interoperable: poseer una estructura diseñada en forma abierta que permita la interconexión con otros sistemas de comando y control, otras fuerzas armadas, agencias del gobiernos y aliados.

Con lo mencionado hasta el momento podemos llegar a la conclusión parcial, que el sistema C^3I^2, cumple la función de mantener los lazos tácticos que le permitan a un comandante conducir sus elementos tanto en el desarrollo de las operaciones tácticas como en su asiento de paz. Es la columna vertebral del sistema de comando y control.

Sección II

Organización de un Centro de Comunicaciones e Informática de Campaña

Concepto General

Los elementos del arma de comunicaciones son los responsables en el establecimiento del sistema de comunicaciones e informático, que brindará apoyo durante las operaciones militares en el nivel CE- TO/TO, Cdo GUB, Cdo GUC, "estableciendo los SCIP del nivel que apoyan. Dichos elementos se organizan para el combate, básicamente, en Centros de Comunicaciones e Informática de Campaña (CCIC)". (Ejército Argentino, 2022, pág. 16)

Un CCIC, está compuesto por personal y medios que tienen la capacidad de transmitir, recibir y distribuir información, en forma de voz, escritos, datos, imágenes y video. Su objetivo principal es brindar apoyo de comunicaciones e informática a puestos comandos de nivel gran unidad, equivalentes y de nivel superior.

Clasificación de los CCIC

En función al puesto comando que brindan apoyo podrán ser:

- Centro de comunicaciones e informática de campaña principal (CCIP), proporcionará apoyo de comunicaciones e informática al puesto comando principal del componente terrestre del teatro de operaciones o a un puesto comando principal de gran unidad (GUB/ GUC).
- Centro de comunicaciones e informática de campaña secundario (CCIS), proporcionará apoyo de comunicaciones e informática al puesto comando de

retaguardia (o secundario) del componente terrestre del teatro de operaciones y a un puesto comando de retaguardia (o secundario) de gran unidad (GUB/ GUC).

- Centro de comunicaciones e informática de campaña de alternativa (CCIA), es eventual y proporcionará apoyo a un puesto comando de alternativa.; en el mismo sentido se determinará el puesto de comunicaciones e informática (PUCOMI) de una unidad para fijar el CCIA de nivel GUC.

Organización

Un centro de comunicaciones e informática de campaña estará, normalmente, constituido por:

a) Elemento para el comando y control del CCIC.

b) Centro de mensajes digital (CMD).

c) Centro de transmisor de video móvil (CTVM).

d) Grupo de ciberdefensa.

e) Terminales satelitales de campaña (TSC).

f) Centro Troncalizador de comunicaciones móvil.

g) Centro de conmutación móvil integrado (CCMI).

h) Elemento para la construcción y mantenimiento de líneas cableadas.

i) Estaciones de radioenlaces digitales de campaña (RDC).

j) Estaciones radioeléctricas y repetidoras de radio.

k) Grupo comunicaciones móvil del puesto comando táctico (GCM/PC).

l) Fracción de seguridad del CCIC.

Sección III

Misiones Particulares y Funciones del Personal

Misiones Particulares

- Jefe de CCIC: conducir los elementos orgánicos y eventualmente agregados, cuando deba instalar y operar el SCIP para permitir el comando y control, a fin de asegurar un continuo apoyo de comunicaciones e informática y una adecuada integración de los sistemas.
- Gpo CMD: diligenciar en forma automática, semiautomática y eventualmente manual los mensajes que ingresen o egresen del CCIC, para procesar el correspondiente diligenciamiento.
- Gpo CCMI: establecer, operar, administrar y mantener sus facilidades integradas e instaladas en el CCIC, para permitir la integración, conmutación y enrutamiento de las redes telefónicas y de transmisión de datos, como así también la interconexión con otras redes o sistemas.
- Gpo RDC: establecer una troncal de alta capacidad para la transmisión y recepción de datos, operando como terminal o repetidor a fin de facilitar la interconexión de facilidades.
- Gpo radioeléctrico: permitir la transmisión y recepción de información de voz y datos, conformando las redes radioeléctricas e integrando los sistemas de comunicaciones e informática.
- Gpo CTVM: constituir un enlace satelital para la transmisión y recepción de imágenes en tiempo real, la integración de los sistemas a la REDISE.
- Gpo construcción y mantenimiento de líneas cableadas: instalar y mantener las líneas físicas telefónicas y de datos, los dispositivos de conectividad

inalámbricos, paneles de conexión y aparatos telefónicos, conectando a su vez las terminales de datos a la red informática en el CCIC.

- Gpo TSC: establecer enlaces en apoyo a distintos medios satelitales fijos y de campaña, a fin de posibilitar su integración a la REDISE.
- Gpo CTCM: brindar apoyo mediante la transmisión, enrutamiento y distribución de voz, datos y videoconferencias, para permitir el acceso a las redes de comunicaciones e informática que posee la Fuerza.
- Gpo GCM/PC: instalar, operar y mantener las facilidades de comunicaciones radioeléctricas, transmisión/recepción de datos, integración radio-cable, integración radio-radio y teléfono satelital, en apoyo al comandante.
- Gpo ciberdefensa: monitorización, que permitan el control y supervisión del CCIC, para asegurar el correcto cumplimiento del Plan CONEM, las normas operativas de tráfico y de empleo de los subsistemas instalados (IEC e IFC) y las políticas de seguridad de informática y de la información.

Funciones del Personal

- Jefe de CCIC: dentro de las principales funciones podemos mencionar la de controlar el sistema con el fin de poder adoptar las medidas correctivas pertinentes, dentro de las atribuciones que se le hayan conferido. Fijar los procedimientos tendientes a la seguridad en las comunicaciones y mantener actualizada la documentación y registros del centro. Como parte del control, deberá supervisar las emisiones de los diferentes grupos radioeléctricos y hacer cumplir estrictamente y hacer cumplir con lo establecido en las Instrucciones para el Funciona- miento de las Comunicaciones (IFC) y en las correspondientes Instrucciones para el Empleo de las Comunicaciones (IEC).

- J Gpo CMD: tendrá la responsabilidad del control y diligenciamiento de los mensajes y la selección de la facilidad más adecuada para su transmisión. Además, supervisará la actualización de toda la documentación correspondiente al puesto y será el encargado de difundir la alarma previamente convenida, a todo el centro de comunicaciones e informática de campaña y al puesto de comando de la gran unidad apoyada.
- J Gpo CCMI: como principal actividad deberá auxiliar al jefe de sección en todo lo referido a la programación de los diferentes circuitos a conectar, coordinará con los jefes de grupo RDC y TSC el diagrama de conexión de los equipos y deberá confeccionar el diagrama de direccionamiento de IP, para la distribución y administración de los datos.
- J Gpo RDC: tendrá dentro de sus funciones la de instalar, operar, mantener y la defensa inmediata de la estación, además coordinará con el jefe del centro de conmutación móvil integrado, el diagrama de circuitos a conectar.
- J Gpo radioeléctrico: controlará el estado de funcionamiento de todos los efectos del equipo, adoptando de inmediato las medidas para subsanar inconvenientes y tendrá la función de transmitir todos los mensajes que lleguen a su grupo.
- J Gpo CTVM: coordinar la instalación de una línea dedicada / exclusiva para tal efecto, y solicitar además la asignación de frecuencias de trabajo en las distintas bandas y los indicativos de llamada, cuando disponga de facilidades para la transmisión de imágenes por radio.
- J Gpo construcciones de líneas cableadas: instalará y mantendrá líneas telefónicas locales internas y externas que enlacen el centro de conmutación del CCIC con abonados en el puesto comando principal del elemento apoyado y los comandos de los elementos dependientes en proximidad al PC. Además,

instalará y mantendrá líneas físicas (cable de campaña, cable UTP, fibra óptica, etc.) para datos y dispositivos de conexión.

- J Gpo TSC: realizar la administración dinámica del ancho de banda satelital disponible y asignar capacidad satelital de acuerdo con prioridad y tiempo de utilización, para permitir el acceso a todas las facilidades de datos disponibles en la REDISE (internet, intranet, correo electrónico, aplicaciones de uso militar y chat).
- J Gpo CTCM: Proporcionar acceso a facilidades de Com e Info a los usuarios apoyados y permitir el acceso a todas las facilidades de datos de la REDISE. Facilitar la integración a las redes radioeléctricas, radioalámbrica, el acceso al sistema informático de transmisión de mensajes y acceder al sistema de videoconferencia de la Fuerza.
- J Gpo GCM/PC: coordinará, con el jefe del CCIC, todos los aspectos relativos al tráfico, desplazamientos previstos, documentación y demás detalles, necesarios para el normal funcionamiento del grupo. Deberá estar en condiciones de satisfacer los requerimientos de comunicaciones que le haga el comandante durante sus desplazamientos fuera del puesto comando principal o de retaguardia.
- J Gpo ciberdefensa: controlar el cumplimiento de las directivas y órdenes que se eleven de los escalones superiores de ciberdefensa. Participar en la detección, registro e identificación de interferencias y/o actividades de engaño que ejecute el enemigo en las redes radioeléctricas del SCIP. Proteger los activos de información, sistemas de información, redes de transmisión de datos, medios de comunicaciones e informática, definidos como críticos y empleados para el comando y control de las operaciones. Ejecutar la búsqueda y detección de

vulnerabilidades en los activos de información, sistemas de información, re- des de transmisión de datos, medios de comunicaciones e informática, definidos como críticos.

Sección IV

Centro de Gravedad

Concepto General

Clausewitz desarrolla el concepto aplicado al medio militar, pero según las traducciones puede variar el sentido, en la traducción trabaja durante la cursada de la especialización, él autor lo interpreta como "un eje de todo poder y movimiento", y mientras que en otras traducciones como "un centro focal". Ambas llevan a pensar en el CDG como una locación más que como una capacidad o característica del enemigo.

En busca de una elaboración más precisa de Centro de Gravedad, lo describe:

> "como el centro de gravedad se encuentra siempre allá donde se concentra la mayor cantidad de masa, y así como cada golpe contra el centro de gravedad de la carga es el más eficaz, y además el golpe más fuerte se consigue con el centro de gravedad de la fuerza, así es en la guerra. Las fuerzas armadas de cada beligerante, ya sea en un Estado o en una alianza de Estados, tienen cierta unidad, y a través de ésta, cohesión; pero allá donde hay cohesión aparecen las analogías con el centro de gravedad. Hay por lo tanto en estas fuerzas armadas ciertos centros de gravedad cuyo movimiento y dirección decide sobre los otros puntos, y estos centros de gravedad se encuentran allí donde se concentra la mayoría de las fuerzas". (Carl Von Clausewitz, 1832, pág. 119)

En nuestra doctrina, el CDG se conceptualiza como las fuentes de poder que otorgan fortalezas o capacidades básicas para poder alcanzar los intereses, objetivos y misiones de un actor.

> “Estas fuentes de poder son subsistemas críticos, que generarán libertad de acción y voluntad de lucha, podrán ser físicos o abstractos y podrán variar con las modificaciones de la situación. La neutralización o afectación de un CDG producirá o contribuirá en forma directa a la desarticulación sistémica propia o del oponente. Una de las actividades esenciales del arte operacional será la determinación del CDG del adversario, concebir cómo neutralizarlo de la mejor manera posible, y definir los propios para poder defenderlos”. (Ejército Argentino, 2015, págs. Anexo 3-2)

Teniendo en cuenta lo mencionado por nuestra doctrina, lo primero que se debe hacer es analizar su sistema como un todo, para poder identificar las conexiones o vacíos que pueda presentar de acuerdo con la situación actual y al ambiente operacional. En la situación donde el enemigo no está lo suficientemente conectado como para actuar como un sistema integral, se deberá analizar como 2 elementos independientes y determinar el CDG para cada uno de ellos.

CDG puede ser inmaterial (voluntad del líder) o algo físico (reservas, centros industriales, líneas de comunicación), por lo que podemos concluir que puede encontrarse en el plano físico, moral y hasta cibernético.

La incorrecta selección de este provocará una incapacidad de lograr el objetivo estratégico a un costo no aceptable y la pérdida injustificada de vidas, materiales y medios.

Los centros de gravedad se pueden atacar/defender de manera directa o indirecta por medio de requerimientos críticos/vulnerabilidades críticas y siempre guarda una relación directa con el objetivo, si cambia el objetivo, se modifica el CGD.

“Está basado en los fines, objetivos, misión y estrategia, decidida por el enemigo. Por lo que debe ser continuamente monitoreado por el equipo C2, tanto en el planeamiento como en la ejecución” (Campos, pág. 177)

Numerosos autores han abordado y tratado diferentes modelos para la identificación y análisis de un CDG, como ser: Jhon Warden, Antulio Echavarria II, Milan Vego, Dale Eikmeire, entre otros, pero a los fines de poder realizar el estudio de las vulnerabilidades críticas de un SCIP, vamos a tomar el planteado por Joseph Strange.

El modelo elaborado por (Strange J. , 2005), realiza una crítica acerca de lo que él denomina una confusión y caos a partir del concepto de Centro de Gravedad que adopta la doctrina conjunta de las FFAA de los EEUU y redefine el concepto y propone un modelo que se basa en la relación siguiente:

- Centro de Gravedad (CDG): Fuentes primarias de moral o la fuerza física, poder y resistencia. No contribuyen a la fortaleza, son la fortaleza.
- Capacidades Críticas (CC): habilidad crítica que identifica al CDG como tal, en el contexto de una situación. Es el elemento que nos dificultaría/Impediría cumplir nuestra misión.
- Requerimientos Críticos (RC): Condiciones Esenciales, Recursos y Medios necesarios para que una CC pueda funcionar efectivamente.
- Vulnerabilidades Críticas (VC): RC o componente del mismo que son deficientes o vulnerables a la neutralización o ataque y lleve a la obtención de resultados decisivos. Impide que el CDG pueda alcanzar su CC.

Puede ser “MORAL, generalmente los líderes, donde su carisma y liderazgo los transforma en CDG Político y Militares, no por la relevancia de su rol, sino por lo que ellos mismos irradian en las fuerzas. También pueden ser FISICOS, los cuales generalmente a nivel estado, serán las FFAA, la industria o el poder económico y ya a Nivel de la Guerra serán las Fuerzas con capacidad para decidir la acción”. (Gniesko, 2017)

Basándome en la doctrina específica del EA y analizando el sistema de comando y control (C^2) de un CTTO, podemos identificar como CDG al sistema de comunicaciones e informática, el cual a este nivel se basa exclusivamente en la instalación, operación y mantenimiento del SCIP. Las diferentes facilidades instaladas, permitirán el desarrollo y normal funcionamiento de otros dos sistemas como ser el C^2 e inteligencia. Por tal motivo su afectación provocará la neutralizaron o degradarán de las actividades básicas de la conducción.

Capacidades, Requerimientos y Vulnerabilidades Criticas del SCIP

Todo CDG, posee ciertas habilidades, fortalezas y recursos fundamentales que son de suma importancia para una organización y se los considera esenciales para proteger y preservar. Estas "capacidades críticas pueden incluir aspectos que van desde el conocimiento, la experiencia y la tecnología ente otras. La identificación y desarrollo es vital para mantener una ventaja competitiva y garantizar la supervivencia a largo plazo". (Strange J. , 1996)

Para la investigación presente y como ya se ha mencionado, el SCIP en apoyo a un CTTO va a ser considerado como el CDG y dentro del método seleccionado sería el primer establecido. Para continuar con su análisis el segundo paso que se debe realizar es la identificación de las capacidades críticas del mismo. Al profundizar en la doctrina del Ejército Argentino podemos concluir que el sistema posibilita la interconexión o integración como punto de acceso, control y diligenciamiento de las comunicaciones, proporcionar seguridad en la transmisión, integrar con los sistemas subsidiarios y la transmisión de videos, televisión y fotografías.

El tercer paso denominado requerimientos críticos, son todos aquellos aspectos considerados necesarios para mantener el equilibrio y la estabilidad del sistema, hace referencia a las condiciones o características que deben cumplirse para que el CDG esté en una ubicación óptima y que garantice el buen funcionamiento de las capacidades críticas.

Tomando como referencia las CC analizadas, podemos identificar y mencionar los siguientes RC: CMD, CCMI, RDC, TSC, medios satelitales, Gpo (s) radioeléctricos, CTCM, GCM/PC, Gpo (s) construcciones de líneas cableadas y el CTVM.

El último paso del método es denominado VC, "son aquellos requisitos críticos, o componentes de los mismos, que son deficientes o vulnerables a la neutralización o degradación de una manera que contribuirá a que un centro de gravedad no logre alcanzar su capacidad crítica". (Strange J. , 1996)

En el caso puntual de un SCIP, se pueden reconocer a las líneas de transmisión, los irradiantes de ondas electromagnéticas, satelitales y de radioenlace, sistemas de alimentación, dispositivos de conectividad informáticos, sistemas informáticos (software), operadores del sistema y los puntos de acceso territoriales.

Una vez identificado las vulnerabilidades críticas, "hay 3 formas de procesos necesarios para atacar la red: saber cómo desarticular, prevenir la reconfiguración y por último evitar la reproducción de la red". (Vera, 2017)

Para poder llevar a cabo los procesos, requiere de la identificación y posterior eliminación de los nodos (SCIP), lugar donde reside la capacidad de coordinación y toma de decisiones.

Tabla 1

Análisis del CDG de un SCIP

Centro de gravedad	Capacidad Crítica
Sistema de comunicaciones e informático particular.	• Punto de acceso (interconexión o integración). • Control y diligenciamiento de las comunicaciones. • Proporcionar seguridad en la transmisión.

	• Apoyo de transmisión de video, televisión y fotografía. • Integrar a los sistemas de comunicaciones subsidiarios.
Requerimiento Crítico	**Vulnerabilidad Crítica**
• CMD. • CCMI. • RDC. • TSC • Medios satelitales. • Gpo (s) radioeléctricos. • CTCM. • GCM/PC. • Gpo(s) construcción de líneas cableadas. • CTVM.	• Líneas de transmisión. • Irradiantes de ondas. Electromagnéticas, satelitales y de radioenlace. • Sistemas de alimentación. • Dispositivos de conectividad informáticos. • Sistemas informáticos (software). • Operadores (del SCIP y PC). • Puntos de accesos territoriales.

Sección V

Conclusiones Parciales del Primer Capítulo

EL puesto comando, desempeña un papel crucial en cualquier operación militar o estratégica. Son centros de control y toma de decisiones donde se coordinan y dirigen las acciones de las fuerzas militares. Al mismo tiempo la importancia de ellos radica en su competencia para recopilar, analizar y transmitir información en tiempo real, lo que permite una toma de decisiones rápida y efectiva.

Los sistemas de comunicaciones son fundamentales para el funcionamiento, permitiendo la transmisión segura y confiable de información entre los diferentes niveles de mando y las unidades en el campo de batalla. La comunicación efectiva es esencial para coordinar las operaciones, compartir inteligencia y mantener la cohesión entre las fuerzas. Se debe agregar, que son una parte fundamental al momento de poder asegurar el cumplimiento

de, “las misiones planteadas y ordenadas, sean realizadas correctamente, y constatar que han logrado el efecto deseado” (Silva, 2019, pág. 24).

El enemigo siempre buscará afectar los puestos comandos y los sistemas de comunicaciones, ya que son puntos clave para debilitar la capacidad de respuesta y la eficacia de las fuerzas enemigas, identificándolos como el centro de gravedad. Pueden intentar interrumpir o interferir las comunicaciones, dañar o destruir los equipos de comunicación, o incluso infiltrarse en los sistemas para obtener información confidencial, con la finalidad de producir daños o una degradación considerable en nuestro C^3I^2.

Por lo tanto, es crucial que estén protegidos y asegurados contra posibles amenazas. Esto implica implementar medidas de seguridad para detectar y contrarrestar posibles ataques cibernéticos, electromagnéticos y físicos.

Este lleva a tener que realizar un análisis profundo de nuestras vulnerabilidades, lo cual nos permitirá prever que nuestro ciclo de reacción tenga la capacidad para soportar ese daño y que se pueda recuperar rápidamente. Hay que mencionar, además que será obtenida por medio de la redundancia, la interconectividad y la interdependencia, las cuales son fuentes de fortaleza que me dará como resultado la resiliencia, “capacidad para soportar daño y recuperarse rápidamente a los intentos de degradación del enemigo”. (Silva, 2019, pág. 25)

Como conclusión parcial de lo ya mencionado en el presente capítulo, se ha podido observar como la evolución de los conflictos, acompañado por los avances tecnológicos, han colocado a los PC y a los CCIC, en el centro de atención de la fuerza enemiga, la cual buscará por todos los medios su neutralización o destrucción.

La protección de estos, antes las acciones de GE y ciberataque, es vital en cualquier operación militar, y su importancia radica en su capacidad para facilitar la toma de decisiones y la coordinación efectiva de las fuerzas.

Capítulo II

Acciones del Enemigo y su Impacto en el Sistema de Comando y Control

En el mencionado capítulo, se abordará el avance de la tecnología y como han surgido nuevas formas de conflicto y amenazas que pueden comprometer la integridad de las comunicaciones y la seguridad de la información. Entre estos desafíos se destacan, la guerra electrónica y los ciberataques.

Ambos temas, representan un riesgo latente para los sistemas de comunicaciones e informática, lo que implica un mayor riesgo de ser blanco de acciones hostiles. La vulnerabilidad de los sistemas de comunicaciones radica en su exposición constante a amenazas externas, así como en las deficiencias en la implementación de medidas de seguridad.

Se llevará a cabo un proceso de comparación y evaluación de las acciones por parte del enemigo, con el objetivo de poder elaborar una matriz de riesgo del sistema de comunicaciones e informático de la fuerza.

Sección I

Acciones de Ciberguerra

Concepto General

Las acciones desarrolladas en este ámbito tendrán un impacto directo en el componente terrestre en diversas perspectivas. Una de ellas es el uso de la fuerza militar convencional como respuesta a un ataque cibernético. Esta posibilidad se considera debido a que los países más poderosos en aplicaciones cibernéticas pueden convertirse en los más vulnerables en este aspecto, porque suelen tener una mayor dependencia de la tecnología y una infraestructura digital más desarrollada. Además, debido a su enfoque en el desarrollo y despliegue de nuevas tecnologías.

Esto implica que pueden priorizar la innovación y la funcionalidad sobre la protección, lo que resulta en vulnerabilidades en sus sistemas. Esto los posiciona en blancos para los ciberataques, ya que un ataque exitoso puede tener un impacto devastador en sus sistemas y en sus operaciones. Los efectos de estos eventos tienen un impacto multiplicador, ya que normalmente su objetivo principal suele ser afectar las infraestructuras críticas.

Por tal motivo, la Directiva de Política de Defensa Nacional (DPDN), establece que el sistema de ciberdefensa debe ejecutar la, "observación, vigilancia y control de la actividad que acontece en la infraestructura de tecnología informática de las redes del Sistema de Defensa Nacional y de las infraestructuras de la información que le sean asignadas, con el fin de prevenir y contrarrestar incidentes provenientes del ciberespacio". (República Argentina - Poder Ejecutivo Nacional, 2021)

En el ámbito del dominio cibernético, se implementan diversas medidas de defensa, tanto activas como pasivas, así como acciones de exploración. Estas estrategias se emplean con el objetivo primordial de salvaguardar las redes y sistemas ante posibles ataques maliciosos. Además, dentro del contexto de las operaciones de información, se utilizan como herramientas para llevar a cabo engaños y desinformación, con la finalidad de crear señuelos o manipular la percepción del enemigo acerca de una determinada situación e inducirlo a tomar decisiones equivocadas, en beneficio de nuestros intereses.

Para poder profundizar sobre el tema, primero se deberá tomar como referencia un concepto específico sobre qué entendemos cuando hablamos de dominio cibernético, para España desde el punto de vista militar "es un dominio global y dinámico dentro del entorno de la información, compuesto por una infraestructura de redes, de tecnologías de información y telecomunicaciones interdependientes, que incluye internet, los sistemas de información y los controladores y procesadores, junto con sus operadores". (Ejército Español, 2013)

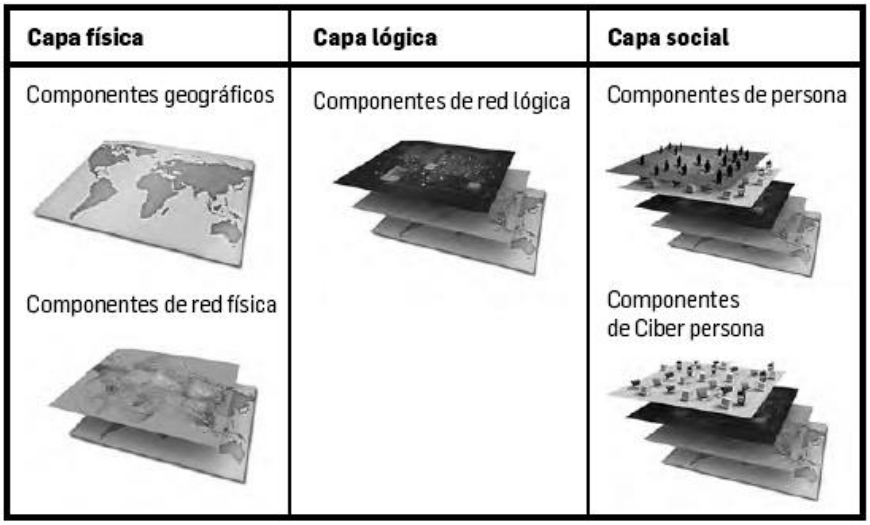
Otra definición es la desarrollada por los Estados Unidos de América, el cual lo define como “el dominio artificial creado al conectar todos los ordenadores, conmutadores, enrutadores, cables de fibra óptica, dispositivos inalámbricos, satélites y otros componentes que nos permiten mover grandes cantidades de datos a velocidades muy rápidas”. (Brett, 2014)

El espacio cibernético también puede ser representado en términos de capas:

- La capa física, es el medio por donde transitan los datos, donde se encuentran los elementos de las redes. Los componentes físicos comprenden el hardware, el software y la infraestructura que apoyan a las redes y a los conectores físicos.
- La capa lógica, consiste en aquellos elementos de la red que se relacionan uno con el otro de manera que se abstraen de la red física, es decir, la forma o las relaciones no están vinculadas a un individuo, ruta de acceso específica o nodo.
- La capa de las ciber – persona, consiste en la gente que se encuentra en un determinado momento presente en la red.

Figura 1

El Espacio Cibernético en Capas - (Joint Publication, 2013)



Operaciones Cibernética

Muchos países del mundo como ser Francia, España y Brasil, han clasificados las operaciones que se llevan a cabo en el espacio cibernético, en acciones defensivas (lucha informática defensiva LID), en acciones de exploración (exploración informática, IE) y en acciones ofensivas (lucha informática ofensiva, LIO).

Las operaciones defensivas son todas aquellas medidas activas y pasivas, que son ejecutadas para mitigar los riesgos y minimizar el impacto de eventuales incidentes de seguridad, a fin de "preservar la libertad de maniobra en el espacio cibernético. Estas acciones son fundamentales para la protección de la infraestructura y los datos frente a las crecientes amenazas, salvaguardando la confidencialidad, integridad y disponibilidad de los sistemas y redes informáticas". (Ejército de la República Federativa de Brasil, 2014)

Las operaciones de exploración se realizan para identificar posibles amenazas y vulnerabilidades en la infraestructura o sistema de información. Las acciones que se realizan tienen por objetivo el desarrollo de estrategias de protección y mejoramiento de la seguridad. Hay que mencionar, además que son fundamentales para fortalecer al sistema, ya que "permiten identificar debilidades y posibles amenazas, brindando la información necesaria para implementar medidas preventivas y de protección más efectivas". (Ejército de la República Federativa de Brasil, 2014)

Las ofensivas, "comprenden las acciones para interrumpir, negar, degradar, corromper o destruir informaciones o sistemas de computación almacenados en dispositivos o redes de computadoras o de comunicaciones del oponente". (Ejército de la República Federativa de Brasil, 2014)

Acciones de Ciberataque

Estas acciones estarán direccionadas hacia las vulnerabilidades críticas que posee nuestro SCIP, las cuales fueron enumeradas por medio del método Strange en el capítulo anterior, para poder ejecutarlas, es necesario llevar a cabo una secuencia de pasos, conocida como “la cadena de un ciberataque”. (Vergara & Trama, 2017)

1. Comprensión: adquirir la información e inteligencia en el ciber ambiente de un blanco del adversario e identificar los objetivos específicos.
2. Desarrollo de la capacidad de carga: desarrollar los códigos de computadora (por ejemplo, malware) que crearán el efecto deseado explotando las vulnerabilidades identificadas del sistema a atacar.
3. Entrega: trasmitir la carga al sistema de destino usando vectores como: adjuntos de correos electrónicos, sitios web y medios extraíbles (por ejemplo, USB).
4. Explotación: después de que la carga haya sido entregada al sistema de destino, la explotación desencadena la carga, explotando una aplicación o una vulnerabilidad del sistema operativo.
5. Instalación: instalar un acceso remoto o puerta trasera en el sistema de destino que permita al adversario mantener una presencia/persistencia dentro del sistema de destino.
6. Mando y control: el adversario establece canales de comunicación para facilitar la transmisión de comandos.
7. Efectos deseados creados: después de progresar a través de las seis primeras fases, el adversario puede tomar acciones para crear los efectos deseados por el atacante.

Todo el planeamiento previo, el análisis y exploración detallada del sistema a afectar, buscando y explotando sus vulnerabilidades, “para interrumpir, negar, degradar, corromper o destruir informaciones o sistemas de computación almacenados en dispositivos o redes de computadoras o de comunicaciones del oponente, persiguiendo los siguientes objetivos”. (López, 2007)

- Propagación de virus computacionales para contaminar el flujo de la información enemiga.
- Controlar los elementos temporales (Internet), tendientes a inducir, engañar, encubrir y contener.
- Interrumpir o sabotear la información o el sistema de información del enemigo, así como su estructura para la conducción de operaciones de información.
- Dispersar las fuerzas, armas y fuegos del enemigo, logrando al mismo tiempo la concentración de las unidades propias.
- Confundir, transmitir información falsa al enemigo y persuadirlo de que lo real es falso y lo falso es real.
- Cambiar los datos en las redes.
- Diseminar propaganda.
- Divulgar información redundante.
- Obtener información.

En función del acceso, el ciberataque puede ser por acceso remoto o por acceso cercano, a través de la colocación local de un determinado hardware o software, obteniendo la capacidad de ingreso al sistema objetivo y lograr los efectos buscados con el ataque, produciendo algunos de los objetivos ya mencionados con anterioridad. Todo esto se podrá llevar a cabo por medio de la ejecución de diversas acciones como ser:

- Ataques de fuerza bruta (Brute Force Attacks): se busca desencriptar contraseñas mediante la combinación de diversas secuencias hasta dar con la correcta.
- Ataques de denegación de servicio (Denial of Service Attacks): se busca colapsar un sistema o red haciendo que el sistema se vuelva inaccesible para los usuarios legítimos.
- Ataques de ingeniería social (Social Engineering Attacks): este tipo de ataque se basa en la manipulación psicológica de las personas para obtener información confidencial o lograr acceso no autorizado a sistemas o redes. Se utilizan técnicas de manipulación y engaño, como el phishing o la suplantación de identidad.
- Ataques de malware (Malware Attacks): se refiere a la infiltración de software malicioso en sistemas o redes con el fin de obtener información confidencial, robar datos o dañar el sistema. Esto puede incluir virus, gusanos, troyanos u otros tipos de software malicioso.

El apoyo de comunicaciones e informática al CTTO, “se materializará mediante la instalación, operación y mantenimiento de redes informáticas que se integrarán y serán parte del ciberespacio, ámbito donde se desarrollarán las operaciones de ciberdefensa”. (Ejército Argentino, 2015, págs. Cap VII - 55)

Como hemos explicado en capítulos anteriores, el SCIP será la materialización del sistema por donde se podrá realizar y ejecutar las actividades básicas de la conducción, dicho de otra manera, será considerado como CDG por parte del enemigo y a través de las diversas acciones que podrá llevar adelante, siendo una de ella el ciberataque, buscará afectar considerablemente al sistema y en consecuencia a los sistemas de comando y control e inteligencia.

Considerando la importancia que representa la preservación y protección de los subsistemas informáticos, será primordial adoptar medidas de seguridad tanto físicas, lógicas, actualización y empleo de procedimientos adecuados para el manejo de la información, las cuales contribuirán a obtener un mayor grado de libertad de acción y asegurar la conducción de las fuerzas terrestres para alcanzar los objetivos establecidos.

Sección II

Acciones de Guerra Electrónica

Concepto General

La GE es una actividad que se desarrolla en un espacio intangible denominado espectro electromagnético, que podemos definir, como el conjunto de todas las frecuencias posibles que producen radiación electromagnética. No todas las ondas electromagnéticas tienen el mismo comportamiento, por ello el espectro electromagnético se divide convencionalmente en segmentos o bandas de frecuencia.

Se refiere al uso de la tecnología y los sistemas electrónicos disponibles para obtener una ventaja significativa en un conflicto militar. Implica la utilización de dispositivos, como radares, sistemas de comunicación, sistemas de vigilancia y contramedidas electrónicas, para detectar, interceptar, interferir y neutralizar las capacidades electrónicas y de comunicación del enemigo. Es parte integral de las operaciones militares modernas, permitiendo alcanzar una superioridad táctica y operativa, al interferir con las capacidades electrónicas y de comunicación del enemigo mientras se protegen las propias.

Según nuestra doctrina, la denominamos como, “cualquier acción que implica el uso de energía electromagnética cuya finalidad esté dirigida a controlar el espectro electromagnético para el empleo efectivo por las propias fuerzas o para atacar al enemigo en este ambiente”. (Ejército Argentino, 2016)

Las operaciones de GE tendrán por objetivo reducir o negar a las fuerzas enemigas la utilización del espectro electromagnético (EEM), contemplando sus comunicaciones y sistemas de armas que utilicen emisiones dentro de este dominio. Al mismo tiempo, poder asegurar el empleo efectivo de los sistemas por parte de las propias fuerzas terrestres.

Las acciones que se ejecutan se pueden clasificar en 3 principales actividades:

- Apoyo de Guerra Electrónica (AGE).
- Ataque Electrónico (AE).
- Protección Electrónica (PE).

AGE: acciones para obtener información, "mediante la búsqueda, interceptación, escucha, localización, análisis, identificación, evaluación y registro de las características de las emisiones detectadas, intencionales o no; con la finalidad de contribuir al inmediato reconocimiento y seguimiento de amenazas presentes en el EEM". (Ejército Argentino, 2016)

AE: comprende el empleo de energía electromagnética para "prevenir o reducir el uso efectivo del espectro electromagnético por parte del enemigo, con la finalidad de afectar negativamente sus sistemas de comunicaciones, sistemas de comunicaciones especiales y sistemas de armas, mediante la ejecución de acciones de interferencia o de engaño". (Ejército Argentino, 2016)

PE: todas aquellas acciones realizadas para proteger al "personal, instalaciones y equipamientos de cualquier efecto producido por el uso del EEM por parte de la propia Fuerza e impedir o reducir la efectividad de las acciones de GE que ejecute el enemigo con la finalidad de degradar, neutralizar o destruir la capacidad propia". (Ejército Argentino, 2016)

En el contexto del empleo de la GE sobre las vulnerabilidades del enemigo, nos enfocaremos sobre las acciones ofensiva. En el campo de batalla moderno, las operaciones de

AE, han demostrado ser un componente vital para debilitar y desestabilizar al enemigo, centrando sus operaciones sobre las vulnerabilidades críticas del adversario.

Otro aspecto clave es la neutralización de los sistemas de defensa del enemigo. Se busca eliminar o minimizar la eficacia de radares, misiles antiaéreos y sistemas de detección mediante el uso de señuelos electrónicos, interferencia electromagnética o interferencia activa. Al debilitar o suprimir las capacidades defensivas, se logra una ventaja estratégica y táctica significativa en el campo de batalla.

Se puede arribar a una conclusión parcial que las acciones de AE, se focalizarán sobre la identificación y explotación de los puntos débiles a través de la perturbación de las comunicaciones y neutralización de los sistemas defensivos.

Los sistemas C^3I^2 en los diferentes niveles de comando se basan en equipos electrónicos que dependen de la radiación electromagnética para poder funcionar correctamente. Estos medios son de suma importancia para el desarrollo de las operaciones tácticas. Por lo tanto, se llevan a cabo diversas actividades con el objetivo de neutralizar o disminuir la efectividad de estos sistemas, buscando afectar negativamente la capacidad de comando y control del enemigo.

Actividades de Ataque Electrónico

Contempla la ejecución de acciones ofensivas, las cuales, para el presente trabajo, es necesario la comprensión y clasificación, para analizar y evaluar el grado de afectación que tienen sobre nuestro CDG, el cual ha sido definido para su estudio al SCIP.

Las actividades de AE en comunicaciones se clasifican en:

1. Interferencia en comunicaciones: “es la radiación, reirradiación o reflexión deliberada de energía electromagnética, con el objeto de impedir / neutralizar o reducir el uso efectivo del espectro electromagnético de los equipos y sistemas de comunicaciones empleados por el enemigo”. (Ejército Argentino, 2016)

2. Engaño en comunicaciones: “es la radiación, reirradiación, alteración, absorción o reflexión deliberada de energía electromagnética, con el objeto de que el enemigo resulte engañado, confundido o sea inducido a obtener conclusiones erróneas de la información proporcionada por sus equipos y sistemas”. (Ejército Argentino, 2016)

Actividades de ataque electrónico en comunicaciones especiales en:

1. Interferencia: es la radiación, reirradiación o reflexión deliberada de energía electromagnética, con el objeto de neutralizar, impedir o reducir la efectividad de radares, sensores, sistemas de armas y/o sistemas de ayuda a la navegación empleados por el enemigo. (Ejército Argentino, 2016)
2. Engaño: “es la radiación, reirradiación, alteración, absorción o reflexión deliberada de energía electromagnética, con el objeto de que el enemigo resulte confundido o sea inducido a obtener conclusiones erróneas de la información proporcionada por sus sistemas”. (Ejército Argentino, 2016)

Es fundamental tener en cuenta las acciones GE sobre nuestro CDG, ya que estas afectarán seriamente nuestra capacidad operativa y nuestra seguridad. Ha quedado demostrado la dependencia cada vez mayor de las tecnologías de la información y comunicaciones, las cuales expone vulnerabilidades que serán explotadas por el adversario. Por tal motivo es de vital importancia generar medidas adecuadas para proteger y fortalecer nuestro SCIP.

Sección III

Nivel de Riesgo del SCIP

Riesgo, en términos generales, se refiere a la posibilidad de sufrir daños, pérdidas o consecuencias adversas como resultado de la exposición a algún tipo de peligro o

incertidumbre. Es una medida, de la probabilidad y magnitud de los efectos no deseados relacionados con una situación o actividad específica.

Para comprender sobre el significado de la palabra, la analizaremos desde el punto de vista de la posibilidad de daño, la probabilidad de que un evento o acción afecte negativamente el cumplimiento de la misión de la fuerza. El riesgo está siempre asociado a una amenaza, aunque la misma puede ser tanto positiva como negativa, es decir, también puede existir la posibilidad de obtener beneficios o resultados favorables al asumir ciertos riesgos, como es en el proceso de toma de decisiones.

En el concepto "se hallan contenido dos elementos básicos para su análisis y evaluación, los cuales son, el impacto y su probabilidad de ocurrencia". (Ejército Argentino, 2022)

La evaluación o análisis de riesgo, es el proceso de conocimiento gradual y analítico de un sistema, que permite conocer y determinar los peligros a los que está expuesto ante la posibilidad de ocurrencia de un evento adverso.

En nuestra doctrina el proceso de evaluación inicia mediante "la identificación del riesgo, para luego poder comenzar con el análisis pertinente, determinar las acciones preventivas o correctivas, ejecutar la revisión de las medidas adoptadas, para finalizar con el control". (Ejército Argentino, 2022)

La identificación consiste en examinar todos los factores que inciden en la situación y que pueden interferir en el cumplimiento de la misión, focalizando en las acciones que ejecute el adversario y como las mismas pueden afectar nuestro CDG y las oportunidades para el logro de los objetivos y en la documentación de algunas de sus características.

Una vez logrado la identificación de los riesgos y su clasificación, es importante "analizarlos teniendo como objetivo central calcular el nivel de amenaza de estos, para poder

priorizarlos y definir cuáles son de mayor importancia, a fin de que se pueda evaluar y plantear las posibles medidas que neutralicen o mitiguen sus efectos". (Etienot, 2014)

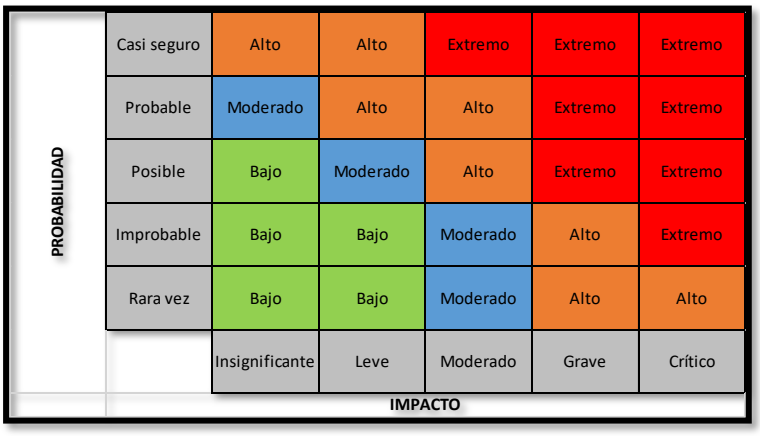
El análisis cualitativo de los riesgos constituye a menudo un medio rápido y rentable para establecer prioridades a la hora de planificar la respuesta a los riesgos o a la hora de realizar el análisis cuantitativo, cuando sea necesario.

La planificación de la respuesta a los riesgos es el proceso de establecer estrategias y acciones específicas para abordar los riesgos identificados. Estas estrategias pueden incluir la mitigación de riesgos, mediante la implementación de "medidas preventivas o de contingencia para reducir la probabilidad o el impacto del riesgo. También pueden incluir la aceptación de riesgos, cuando el impacto se considera insignificante o la oportunidad de aprovechar los riesgos, cuando se identifican posibles beneficios". (Etienot, 2014)

La supervisión y el control de los riesgos evalúan la eficacia de todo el proceso de gestión y desencadenan acciones correctivas y preventivas. Se establecen mecanismos para monitorear y controlar la implementación de las estrategias en respuesta a los mismos. Esto puede implicar la revisión regular del plan de acción, la actualización en función de los cambios en los riesgos o la evaluación del impacto de las acciones implementadas.

Figura 2

Matriz de Exposición de Riesgo



Tomando como referencia el concepto de riesgo desarrollado en el presente capítulo, la evaluación es crucial para comprender nuestras vulnerabilidades y prepararnos contra las amenazas que se podrán materializar en un conflicto armado.

Analizando nuestro CDG, se puede identificar las diferentes vulnerabilidades críticas que presenta nuestro SCIP y ante la probabilidad de ocurrencia de operaciones de GE y ciberataques a nuestros sistemas, es sumamente importante priorizar las medidas que se deberán adoptar, a los fines de disminuir los efectos o impacto de las acciones enemigas.

Tabla 2

Identificación de Amenazas

Vulnerabilidad Crítica	Identificación de amenaza
• Irradiantes de ondas. Electromagnéticas, satelitales y de radioenlace. • Dispositivos de conectividad informáticos. • Sistemas informáticos (software).	• Puertas traseras. • Malware. • Ataque a las conexiones. • Interferencia electrónica.
• Sistemas de alimentación. • Operadores (del SCIP y PC). • Líneas de transmisión. • Puntos de accesos territoriales.	• Ingeniería social • Sabotaje. • Engaño. • Falta de capacitación de los operadores.

Es importante comprender que las vulnerabilidades críticas mencionadas en la Tabla 2, son todos aquellos problemas conocidos sobre nuestros sistemas, que por diversas razones no han sido solucionadas y se convierten en debilidades que podrán ser aprovechadas y explotadas por nuestros enemigos.

Nuestros adversarios según la materia de Estrategia y Pensamiento Militar Contemporáneo se pueden clasificar en países de primer, segundo, tercer y cuarto orden. Los

de primer y segundo orden, son todos aquellos que poseen un poderío militar significativo y que cuentan con fuerzas armadas bien equipadas y capaces de proyectar su poder tanto a nivel regional como global. Estos países principalmente tienen una economía grande y desarrollada, con un alto gasto militar, una amplia capacidad de producción de armamento, tecnología militar avanzada y poder nuclear. La diferencia entre ambos está dada en la cantidad de medios militares.

Un país de tercer orden generalmente posee una capacidad militar limitada, es decir, un ejército más pequeño, menos sofisticado y con una probable dependencia de ayuda o cooperación de países más fuertes en caso de enfrentar amenazas militares significativas. Tienen una disminuida influencia y poder militar, y suelen ser vistos como menos relevantes en el escenario mundial.

El término de país de cuarto orden es aún más débil y menos capaz militarmente que los países de tercer orden. Estos estados tienen fuerzas armadas reducidas, recursos limitados y dependencia casi total de la ayuda de países más fuertes en caso de conflicto militar.

A lo expresado anteriormente hay que agregar la existencia de actores cibernéticos conocidos también por la sigla ATP (Advanced Persistent Threat), “son individuos o grupos coordinados que atacan a personas u organizaciones con el fin de obtener ganancias personales, nacionales, sociales o políticas”. (Easydmarc, 2021)

Los ataques que ejecutan son una amenaza, cuyo principal problema es la dificultad de detección temprana, ya que los atacantes utilizan diferentes técnicas, tanto para permanecer el mayor tiempo posible sin ser detectados, como para evadir de manera eficiente los sistemas de seguridad.

Pueden estar respaldados o actuar en nombre de un gobierno, los cuales los pueden utilizar como una herramienta para alcanzar sus objetivos en sectores como la defensa nacional,

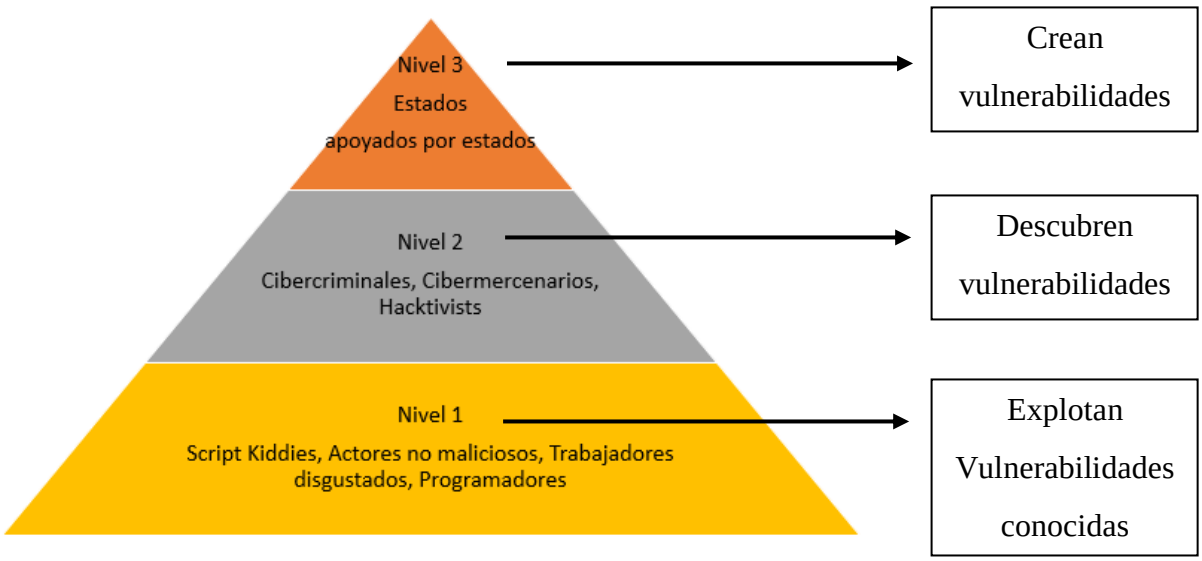
sector industrial, ya que pueden acceder a información de alto valor, planes militares y otros datos de relevancia de los gobiernos y otras organizaciones.

La relación entre los actores cibernéticos y los estados puede ser compleja y variada, en algunos casos, los gobiernos pueden patrocinar directamente a grupos o individuos que actúan en forma indirecta en nombre ellos, proporcionándoles, recursos técnicos, financieros o legales, lo que permite tener acceso a información privilegiada o a herramientas y técnicas sofisticadas que les permiten llevar a cabo ataques cibernéticos de gran envergadura.

También pueden ser utilizados como una táctica de guerra, conocida como ciberwarfare. En lugar de recurrir a conflictos militares convencionales, los estados pueden optar por utilizar las capacidades cibernéticas para dañar las infraestructuras críticas, interrumpir sistemas de comunicación o robar información confidencial, permitiendo a los actores de primer, segundo, tercer y cuarto orden evadir responsabilidades sobre las acciones ejecutadas. Esto genera un entorno de impunidad en el ciberespacio y dificulta los esfuerzos para mantener la seguridad y estabilidad.

Figura 3

Clasificación de los Actores Cibernéticos



Fuente: Dirección de Ciberdefensa del Ejército Argentino.

Al trasladar las amenazas identificadas a nuestra matriz de riesgo, es casi seguro que el enemigo intente aprovechar nuestras vulnerabilidades, especialmente en relación con los países de primer y segundo orden, así como a los actores cibernéticos de nivel 3. Sin embargo, también existe una probabilidad de riesgo significativo cuando se trata de los países de tercer y cuarto orden, al igual que los actores de nivel 2 y 1.

Tomando la posibilidad de agresión más peligrosa, el impacto que producirían las acciones de nuestro adversario sobre nuestro SCIP, nos da como resultado un riesgo extremo / alto.

Sección IV

Conclusiones Parciales del Segundo Capítulo

El aumento de las operaciones de GE y ciberataques ha llevado a un incremento significativo de los riesgos para nuestros sistemas de comunicación e informático. Estas acciones están diseñadas para obtener acceso no autorizado, robar información confidencial, interrumpir servicios críticos, causar daños a infraestructuras críticas, interferir en el sistema de comando y control e inteligencia.

Pueden causar una neutralización en las facilidades esenciales para la conducción de operaciones militares, como el suministro de energía, las comunicaciones y la afectación de los servicios informáticos.

Los costos asociados con la recuperación de los sistemas afectados, la reparación de infraestructuras dañadas, las perdidas en vidas humanas y la mitigación de las consecuencias pueden ser enormes.

Las amenazas no solo son llevadas a cabo por actores estatales, sino también por grupos terroristas, organizaciones criminales y hackers individuales. Esto hace que sea aún más difícil

prevenir y minimizar estos riesgos, ya que los perpetradores pueden ser difíciles de identificar y rastrear.

En resumen, las acciones de GE y ciberataques representan una amenaza cada vez mayor para nuestros sistemas y requieren una respuesta proactiva para proteger nuestra infraestructura crítica y nuestra información confidencial. La conciencia de estos riesgos y la implementación de medidas de seguridad sólidas, son esenciales para combatir esta creciente amenaza.

Capítulo III

La Seguridad del Sistema de Comunicaciones e Informático Particular

En el presente capítulo explicaremos cómo la seguridad es un factor esencial en la protección de la información, la cual es una herramienta útil en la toma de decisiones de una organización, debido a su valor incalculable y a su importancia, por tal motivo es imprescindible protegerla adecuadamente.

El avance de la tecnología crece a pasos agigantados y con ello su perfeccionamiento y sofisticación, puntualmente en él campo de las comunicaciones y su capacidad de conexión con otros dispositivos remotos y físicamente separados. Si la información no se encuentra debidamente resguardada durante su utilización, almacenamiento y en su proceso de transmisión, puede ocasionar perdidas verdaderamente significativas, generando riesgo e incertidumbre en la exactitud de esta, por ello es muy importante desarrollar políticas de seguridad claras con la intención de mantener protegida las comunicaciones durante el proceso de emisión, transporte y recepción.

Teniendo en cuanta lo antes mencionado, se elaborará un análisis y evaluación de la seguridad establecida en un SCIP, para así poder identificar las acciones a corregir, con el propósito de erradicar o minimizar nuestras vulnerabilidades y permitir un adecuado comando y control de las operaciones.

Sección I

Seguridad en las Comunicaciones

La seguridad expone un estado de protección contra posibles daños, riesgos o peligros que puedan afectar a las personas, bienes, información o cualquier otro activo valioso. Es un concepto amplio que abarca diferentes aspectos, como la seguridad física, la seguridad informática, entre otros.

En términos generales, busca minimizar los efectos de las amenazas y riesgos, así como prevenir incidentes que puedan poner en peligro la integridad o el funcionamiento adecuado de los elementos protegidos. Esto se logra mediante la implementación de medidas preventivas, como sistemas de vigilancia, controles de acceso, protocolos de seguridad, capacitaciones y por medio de medidas activas / reactivas tanto en GE como en ciberdefensa.

En el ámbito de las comunicaciones militares, se refiere a las medidas y protocolos que se toman para proteger la información transmitida a través de diferentes medios de comunicación, como internet, las redes de telefonía fija, móvil y satelitales y los sistemas radioeléctricos.

Su importancia radica en que la información transmitida puede tener clasificación reservada, confidencial o secreta. Sin las medidas adecuadas, esta información puede ser interceptada o comprometida por las acciones del enemigo.

La relación entre la seguridad y las comunicaciones exige precisar conceptos rectores que determinen una integración armónica y coordinada entre ambas. Cuando hablamos de seguridad de las comunicaciones, debemos interpretar como la “protección resultante de todas las medidas destinadas a negar al oponente la información de valor que pueda ser extraída de la interceptación, escucha y análisis de las comunicaciones”. (Ejército Argentino, 2014, págs. VIII - 2)

La seguridad en las comunicaciones describe a las “medidas y controles para denegar el acceso a través de las redes a entidades no autorizadas, así como para garantizar la autenticidad de las partes en comunicación”. (Ejército Argentino, 2014)

Mientras que la seguridad en la transmisión, “deriva de la elección de los medios y métodos de comunicaciones que mejor respondan al propósito de impedir la interceptación del tráfico propio y su posterior análisis”. (Ejército Argentino, 2014)

Por tales motivos las medidas que se deben adoptar comprenderán, “la protección de las emisiones de comunicaciones y de comunicaciones especiales, el tráfico y el empleo de facilidades, como también así su método operativo”. (Ejército Argentino, 2016)

En lo que respecta a la protección, se debe entender como el conjunto de medidas y acciones que se implementan con la finalidad de negar la obtención de información a través de la interceptación de las emisiones electromagnéticas que sean emanadas de las diferentes facilidades instaladas dentro de un SCIP. Buscando el efecto de neutralizar o disminuir las actividades de AE por parte del enemigo contra nuestros sistemas de comunicaciones e informática y los sistemas de armas.

Para alcanzar el cumplimiento de los objetivos, la Fuerza ha implementado una serie de medidas y acciones tendientes a brindar la seguridad necesaria, que garantice el normal funcionamiento de los sistemas de comando y control e inteligencia, siendo las de mayor importancia:

1. Control de emisiones.
2. Evasión de emisiones.
3. Adiestramiento del personal en técnicas y procedimientos.
4. Elaboración de informes al comando superior sobre la detección de actividades de GE del enemigo.
5. Llevando un registro actualizado sobre las interferencias reconocidas.
6. Órdenes técnicas para el control de frecuencias.
7. Todas las medidas de protección incorporadas en los equipos.

Al analizar y evaluar nuestro sistema de comunicaciones y a los fines que el mismo sea confiable y seguro, realizaremos una comparación entre las amenazas identificadas en nuestra

matriz y las acciones establecidas doctrinalmente para la protección del tráfico y el empleo de las facilidades y métodos operativos de transmisión.

Tabla 3

Comparación entre Amenazas y Medias de Protección

Identificación de amenaza	Protección del tráfico	Protección por empleo de facilidades y métodos.
• Puertas traseras. • Malware. • Ataque a las conexiones. • Interferencia electrónica. • Ingeniería social • Sabotaje. • Engaño. • Falta de capacitación de los operadores.	• Elaborar normas operativas de tráfico. • Aprendizaje por parte de los operadores sobre las normas. • Cumplimiento de las normas y procedimientos. • Cumplimiento de los criterios de emisión. • Empleo de sistemas de autenticación. • Adecuado uso y control de frecuencias. • Empleo de sistemas contra la interferencia y engaño. • Aplicación de seguridad criptográfica. • Correcto diligenciamiento de los mensajes. • Correcto empleo de los equipos.	• Correcta selección de la facilidad más adecuada. • Cumplimiento del plan control de emisiones (CONEM). • Ejecutar procedimientos de evasión de emisiones. • Las facilidades cuenten con sistemas de protección incorporados.

Amenazas del ámbito informático y electromagnético.

Amenazas del ámbito de capacitación profesional.

Medidas que no son implementadas en forma correcta.

Uno de los problemas que se ha presentado en la actualidad, es la rapidez con que se suceden y desarrollan nuevas tecnologías, lo cual conlleva su pronta obsolescencia y obliga a establecer un compromiso en la modernización o renovación de los sistemas, equipos, procedimientos y capacitación de los operadores.

Comparando las medidas adoptadas y teniendo en cuenta las amenazas, podemos identificar que ciertas medidas de protección no son adecuadas y otras no se cumplen en forma eficiente, dejando a nuestro sistema vulnerable a las acciones de GE y ciberataques del enemigo.

La transmisión de información clasificada constituye un momento crítico, durante el proceso de transmisión de los documentos que la contienen, por cuanto en esa oportunidad se incrementan las posibilidades de su interceptación por parte del enemigo. Por tal motivo, el personal deberá tener presente que las comunicaciones podrán ser susceptibles a los efectos de las operaciones del adversario, sin importar el enlace que se utilice.

Al momento de establecer una medida para contrarrestar una amenaza, se puede contemplar facilidades que posean capacidades de protección incorporados, exigiendo el empleo de medidas contra la interferencia, engaño y aplicación de seguridad criptográfica. Esto nos lleva a pensar, si realmente la solución de esa falencia en la seguridad está dada por la simple adquisición de quipos que posean las mencionadas capacidades.

La elaboración de normas, acompañado por un ciclo de aprendizaje de los operadores, que le brindará los conocimientos necesarios para poder instalar, operar y mantener el equipo en condiciones óptimas de funcionamiento, es otro aspecto en el cual podemos identificar deficiencias en cuanto al nivel de capacitación adquirido por el personal para cumplir en forma eficiente su rol de combate dentro de un elemento de comunicaciones según el perfil profesional requerido para tales fines.

Sección II

Seguridad Informática

Cuando hablemos de seguridad informática podemos interpretarla como la protección de la información y de los sistemas informáticos, para garantizar su confidencialidad, integridad y disponibilidad. Lo cual incluye la implementación de medidas preventivas y reactivas, para proteger los sistemas contra amenazas, como ser el acceso no autorizado, el robo de datos, el malware y los ataques cibernéticos.

Los activos de información que posea la Fuerza, es el principal objetivo por proteger contra posibles amenazas. Son todos aquellos elementos de importancia en "la producción, emisión, almacenamiento, comunicación, visualización y recuperación de información de valor". (Ejército Argentino, 2016). Comprende a la información como tal, en sus diferentes formatos, a los equipos, sistemas informáticos y software y por último a las personas que manipulan información.

Un incidente de seguridad informática es un evento adverso que compromete la confidencialidad, integridad o disponibilidad, la legalidad y confiabilidad de la información y los recursos tecnológicos. Puede ser causado mediante la explotación de alguna vulnerabilidad o un intento o amenaza de romper los mecanismos de seguridad existentes.

Los accesos no autorizados se podrán clasificar en, (Ejército Argentino, 2014)

1. Accesos no autorizados exitosos.
2. Robo de información.
3. Borrado de información.
4. Alteración de la información.
5. Intentos recurrentes y no recurrentes de acceso no autorizado.

6. Abuso y mal uso de los servicios informáticos internos o externos que requieren autenticación.

Con la finalidad de proteger el sistema de las acciones del enemigo, el proceso de seguridad deberá ser continuo y cíclico, abarcando tres áreas fundamentales como ser: la física, la lógica y la administrativa.

La seguridad física se refiere a la protección de los activos físicos relacionados con la información y sistemas informáticos. Esto incluye la protección de equipos, servidores, centros de datos, cableado y cualquier otro componente físico involucrado en los sistemas informáticos. Se enfoca en prevenir el acceso no autorizado, el robo, el daño físico o la manipulación de estos activos. Es esencial para garantizar la confidencialidad, integridad y disponibilidad de la información y los sistemas informáticos.

La seguridad lógica, también conocida como seguridad de la información, se centra en proteger la información y los sistemas de una organización a través de medidas de seguridad tecnológicas. Se enfoca en la protección de los datos y el software de una computadora o de una red de computadoras, para salvaguardar la confidencialidad, integridad y disponibilidad de la información. Esto implica implementar controles y políticas de seguridad, asegurando los datos contra accesos no autorizados, modificaciones no deseadas o pérdida accidental o intencional. Algunas medidas comunes de seguridad lógica incluyen:

- Autenticación: Verificar la identidad de los usuarios.
- Control de acceso: Limitar el acceso a los recursos informáticos solo a personas autorizadas.
- Encriptación.
- Firewall: Un sistema de seguridad que controla el tráfico de red y protege la red.
- Detección y prevención de intrusiones.

- Auditoría y monitoreo: Supervisar y revisar los registros de eventos.

La seguridad administrativa se refiere a las medidas y prácticas implementadas para proteger los activos de información de una organización a través de la gestión adecuada de los recursos humanos, las políticas y los procedimientos. Esto implica establecer roles y responsabilidades claramente definidos dentro de la organización, así como implementar políticas y procedimientos de seguridad informática. Algunas de las actividades clave que se realizan en el ámbito de la seguridad administrativa son:

- Gestión de usuarios y accesos: se encarga de definir quiénes tienen acceso a los sistemas y datos de la organización, así como de qué manera pueden acceder a ellos.
- Políticas y procedimientos: se deben establecer políticas claras que dicten cómo deben utilizarse los recursos de información de la organización y cómo se deben manejar los incidentes de seguridad.
- Supervisión y auditoría: es necesario llevar a cabo monitoreo constante de los sistemas y actividades de los usuarios para detectar cualquier comportamiento anómalo o incumplimiento de las políticas de seguridad.
- Capacitación y concientización: es fundamental brindar a todos los miembros de la organización la capacitación adecuada en seguridad informática, para que estén al tanto de los riesgos y amenazas y sepan cómo manejarlos de manera segura.

En la actualidad, los ciberataques están en constante aumento y se vuelven cada vez más sofisticados y difíciles de combatir. Por esta razón, resulta fundamental que nuestro SCIP cuente con un área dedicada a la seguridad informática y disponga de herramientas que garanticen la confiabilidad de nuestras redes y operaciones. De esta manera, podremos contar

con la tranquilidad de saber que nuestras actividades se desarrollan de forma segura y con una mínima posibilidad de sufrir algún tipo de ataque.

Una gran parte de los datos que resguarda un puesto comando es información confidencial, donde el acceso es restringido y su exposición no está autorizada. Pese a esto, la transmisión de datos confidenciales se da a través de redes y otros dispositivos, donde la seguridad informática es necesaria, pues se encarga de proteger esa información y los sistemas utilizados para procesarla y almacenarla.

Por lo antes precitado, es menester reevaluar nuestro sistema de seguridad informático, el cual exhibe diversas debilidades manifiestas en nuestro SCIP. Si estas falencias no son atendidas adecuadamente, se convertirán en vulnerabilidades susceptibles de ser explotadas por aquellos que nos adversan.

Tabla 4

Vulnerabilidades Detectadas en un SCIP - (Morales, 2022)

Nro	Activo	Vulnerabilidades	Descripción	Contramedidas
1	**Panasonic CF-19**	Controlador de WAN inalámbrica (Sierra Wireless) (CVE-2020-8948)	Los paquetes de controladores de Sierra Wireless antes de la compilación 5043 permiten a un usuario sin privilegios sobrescribir archivos arbitrarios en carpetas mediante vínculos físicos. Un usuario sin privilegios podría aprovechar esta vulnerabilidad para ejecutar código arbitrario con privilegios del sistema.	Actualizar a la versión 5043 MDBP o posterior.
		Vulnerabilidad al instalar Intel Wireless Drivers y software relacionado (WiFi/Bluetooth/W	La vulnerabilidad de inyección de DLL en los ejecutables de instalación (Autorun.exe y Setup.exe) para los controladores	Intel recomienda enfáticamente que los usuarios con controladores afectados

Nro	Activo	Vulnerabilidades	Descripción	Contramedidas
		API) (CVE-2018-3649)	inalámbricos de Intel y el software relacionado permite que un atacante local provoque una escalada de privilegios a través de la ejecución remota de código.	descarguen y actualicen al controlador compatible más reciente.
2	**ROUTER: CCMI, RDC: CISCO 2901**, Software/Firmware: 15.4 configuración una placa F/E de 4 puertos, una placa FXS 4 internos.	Cisco anuncia las fechas de finalización de la venta y de la vida útil del software Cisco Select ISR 1900, 2900 y 3900. (Boletín EOL14566)	Después del 31 mayo 2027, todos los servicios de soporte para el producto dejarán de estar disponibles y el producto quedará obsoleto.	Renovar equipamiento a modelos más nuevos con soporte por parte del fabricante.
		Los enrutadores ISR G2 no responden al comando de secuencia de ruptura de recuperación de contraseña.	Los enrutadores con ROMMON versión 15.0(1r) M1 no responden al comando de secuencia de interrupción recibido de un dispositivo conectado al puerto de la consola. Esta falla impide la recuperación normal de la contraseña del dispositivo. (Ctrl+Break)	Se recomienda actualizar el software.
3	**ROUTER: TSCR: CISCO 1700 Series** (sin acceso a datos de firmware ni configuración).	Cisco IOS 12.0 a 12.4 vulnerable. (CVE-2007-4293)	Cisco IOS 12.0 a 12.4 permite a los atacantes remotos causar una denegación de servicio a través de mensajes en el protocolo de voz MGCP.	Se recomienda actualizar el software Cisco IOS.
		Cisco IOS 12.0 a 12.4 e IOS XR anterior a 3.2 vulnerable. (CVE-2005-2451)	Cisco IOS 12.0 a 12.4 e IOS XR anterior a 3.2, con IPv6 habilitado, permite a atacantes remotos en un segmento de red local provocar una denegación de servicio por sobre carga del dispositivo, y posiblemente ejecutar código arbitrario a través de un paquete IPv6 manipulado.	Se recomienda actualizar el software Cisco IOS o deshabilitar conexiones IPv6.

Nro	Activo	Vulnerabilidades	Descripción	Contramedidas
		Desbordamiento de búfer en la funcionalidad del Protocolo NHRP en Cisco IOS 12.0 a 12.4. (CVE-2007-4286)	Permite a los atacantes remotos provocar una denegación de servicio por reinicio y ejecutar código arbitrario a través de un paquete NHRP manipulado. Este protocolo está en la capa de enlace de datos y se utiliza para mapear dinámicamente una dirección IP a la interfaz de los otros sistemas que forman parte de la red, permitiendo que estos sistemas se comuniquen directamente.	Se recomienda actualizar el software Cisco IOS.
4	**Switch (Capa 2) TSCR**: 3Com Baseline 2016 3C164	Firmware vulnerable en versiones anteriores a 1.0.2.0. (CVE-2006-2054)	3Com Baseline Switch 2848-SFP Plus Modelo #3C16486 con firmware anterior a 1.0.2.0 permite a atacantes remotos provocar una denegación de servicio (operación inestable) a través de paquetes DHCP.	Descargar firmware versión 1.0.2.0
5	**Antenas Wireless Motorola: PTP58300** ODU Mod WB 3163 Versión Firmware 2000-2010	El cnMaestro local es vulnerable. (CVE-2022-1361)	El cnMaestro local afectado es vulnerable a una filtración de datos previa a la autenticación a través de la neutralización incorrecta de elementos especiales utilizados en un comando SQL. Esto podría permitir a un atacante filtrar datos sobre las cuentas y dispositivos de otros usuarios.	Descargar firmware versiones posteriores al 2010.
6	**Antenas Wireless**	El cnMaestro local es vulnerable. (CVE-2022-1360)	El cnMaestro local afectado es vulnerable a la ejecución de código en el servidor de alojamiento cnMaestro. Esto podría permitir que un atacante remoto cambie los ajustes de	Descargar firmware versiones posteriores al 2010.

Nro	Activo	Vulnerabilidades	Descripción	Contramedidas
			configuración del servidor.	
7	**Motorola: PTP58300** ODU Mod WB 3163 Versión Firmware 2000-2010	El cnMaestro local es vulnerable. (CVE-2022-1359)	El cnMaestro local afectado es vulnerable a una escritura de archivo arbitraria a través de una limitación incorrecta de un nombre de ruta a un directorio restringido. Esto podría permitir que un atacante escriba datos en cualquier archivo del servidor.	Descargar firmware versiones posteriores al 2010.
8	**Antenas Wireless**	El cnMaestro local es vulnerable. (CVE-2022-1358)	El On-Premise afectado es vulnerable a la exfiltración de datos a través de la neutralización inadecuada con comandos SQL. Esto podría permitir que un atacante extraiga y descargue todos los datos almacenados en la base de datos cnMaestro.	Descargar firmware versiones posteriores al 2010.
9	**Sistema de Comando y Control**	Datos sin cifrar	Los datos se transmiten en claro salvo que sean cifrados por el sistema del equipo de radio	Cifrar los datos con sistemas simétricos y/o asimétricos.

Cuando nos referimos a la planificación de seguridad que realiza la fuerza, podemos observar una notable falta de cumplimiento de las diferentes medidas por parte de los organismos encargados, debido a diversos factores. Uno de ellos es el desconocimiento de las directivas por parte de los responsables, lo cual impide que se sigan correctamente los protocolos establecidos.

Otro factor es la falta de compromiso de la cadena de comando, al no llevar a cabo los controles necesarios en los niveles inferiores, para asegurar que se estén siguiendo e implementando correctamente las medidas de seguridad establecidas. Además, la falta de

capacitación y concientización de los operadores, también inciden en esta carencia, esta falencia en la ejecución de los procedimientos conlleva a que no se cumplan con las medidas de manera adecuada y expone al sistema a numerosos riesgos de fuga de información y quedar expuesto a las acciones del enemigo.

Esta es la razón por la que deben priorizarse las acciones orientadas a enfrentar y prevenir cualquier tipo de ciberataque ocasionado por Estados, hackers e incluso aplicaciones basadas en Inteligencia Artificial programadas para el robo sistemático de datos.

A las mencionadas falencias identificadas, se debe sumar la utilización de software gratuito y no oficial, los cuales pueden contener malware o virus ocultos que pueden dañar o comprometer la seguridad del sistema.

Generalmente, no reciben actualizaciones regulares de seguridad. Esto significa que no se solucionarán vulnerabilidades conocidas, ni se parchearán agujeros de seguridad, lo que lo deja expuesto a posibles ataques, a los que se le suma la falta de soporte técnico y la poco concientización y falta de capacitación de los operadores.

Sección III

Conclusiones Parciales del Tercer Capítulo

La falta de implementación de las medidas de seguridad de comunicaciones e informática o su empleo parcial por diversas causas, pueden tener graves consecuencias. En primer lugar, la filtración de información sensible puede comprometer la seguridad, permitiendo que enemigos accedan a datos estratégicos, tácticos o de inteligencia. Esto podría darles ventaja en el campo de batalla.

Además, puede hacer que los sistemas militares sean susceptibles a ataques cibernéticos. Estos ataques pueden afectar directamente la operatividad de las fuerzas armadas, interrumpiendo las comunicaciones, desactivando sistemas de armas o dañando infraestructuras

críticas. Esto generaría un grave impacto en la capacidad de defensa y podría debilitar la capacidad militar de un país.

Otro riesgo asociado es el uso indebido de la información militar por parte de actores malintencionados. Esto podría incluir el robo de información o su manipulación para engañar a las fuerzas armadas y generar confusiones en el campo de batalla.

En resumen, contar con medidas de seguridad de comunicaciones e informática en el ámbito militar es esencial para garantizar la seguridad nacional y la defensa de un país. La no implementación de estas medidas puede tener consecuencias desastrosas, comprometiendo la confidencialidad de la información, permitiendo ataques cibernéticos y poniendo en peligro la capacidad de defensa. Es necesario invertir en tecnología y capacitación para garantizar la protección de la información y los sistemas militares.

Conclusiones Finales

Luego de haber realizado una profunda investigación sobre la seguridad del SCIP de un CTTO, reconociendo al mismo como el CDG de las acciones a ejecutar por el enemigo, con la finalidad de afectar el comando y control de las operaciones, podemos arribar a una posible respuesta a nuestro interrogante planteado al inicio del proyecto, el cual plantea la problemática sobre cuáles son las acciones por adoptar para asegurar un ágil, seguro y confiable sistema de control.

Como primer paso para poder arribar a una respuesta lo más precisa, se realizó un estudio sobre el sistema de comunicaciones e informática, su organización, misiones particulares y funciones de sus integrantes, con el objetivo de llevar adelante un análisis y posterior evaluación del sistema como CDG, con la finalidad de identificar sus vulnerabilidades críticas.

El segundo paso obligado estuvo centrado en la comparación de nuestras VC con las acciones de ciberataques y GE perpetradas por parte del enemigo, entendiendo el riesgo que representan y el impacto negativo que poseen sobre nuestro sistema instalado y sus efectos sobre las actividades básicas de la conducción. Lo cual permitió elaborar una matriz de riesgo, obteniendo e individualizando las amenazas en relación con nuestras vulnerabilidades.

Una vez identificadas y definidas las amenazas, se realizó un análisis y evaluación en forma integral, con las medidas de seguridad de comunicaciones e informáticas existentes en nuestra doctrina y su aplicación física, lógica, administrativa, como así también los procedimientos relacionados con su aplicación.

El resultado de este exhaustivo proceso nos llevó a varias conclusiones sobre nuestro sistema actual, el cual requiere modificaciones y la implementación de acciones específicas

para garantizar su integridad frente a cualquier agresión enemiga. Solo así podremos garantizar la protección de nuestras operaciones en un entorno cada vez más hostil.

Las acciones que se van a proponer se pueden agrupar en tres grandes grupos, uno referido a los equipamientos, el otro relacionado con la capacitación de los operadores y el último relacionado a las directivas de seguridad informáticas.

Abordando el primer grupo, el de equipamiento, en los últimos años, hubo un incremento notable en materia de inversión, podemos aludir a la incorporación de materiales tecnológicos, pudiendo citar, las facilidades radioeléctricas con capacidades de transmisión de voz y datos, encriptado y salto de frecuencia bajo normas MIL, el HF Falcon III RF-7800 de la empresa Harris Corporation de origen estadounidense. Su operatividad no solo se limita a las facilidades de emisiones radioeléctricas clásicas, sino también a la operación informática.

Respecto a la adquisición mencionada, se podría argumentar que la Fuerza puede llegar a creer que ha obtenido un sistema seguro y confiable. No obstante, la realidad es que, al tratarse de un equipo fabricado en el extranjero, es comprensible tener ciertas dudas acerca de la existencia de posibles puertas traseras que pudieran facilitar el desencriptado de las comunicaciones en caso de un conflicto de intereses.

Un ejemplo práctico, es lo sucedido recientemente, donde el Ministerio de Defensa Australiano, cancelo el contrato sobre el sistema de comando y control de Elbit, procedente de Israel. Los motivos de la decisión tomada radican principalmente en dos causas, la primera adjudicada a los costos elevados pero la segunda es la “detección de puertas traseras en el sistema que supondrían una vulnerabilidad de la seguridad del sistema y durante los últimos doce meses, el sistema habría tenido dos fallos importantes de seguridad”. (García, 2021)

Un caso notable que ejemplifica la problemática asociada a la adquisición de equipamiento extranjero, como podría ser el caso de los medios con capacidad de encriptación,

se encuentra en el incidente conocido como Crypto AG. Dicho suceso constituyó un escándalo de espionaje que tuvo implicaciones con una empresa suiza dedicada al cifrado de información.

Crypto AG estaba siendo controlada en secreto por la Agencia de Inteligencia de Estados Unidos (CIA) y el Servicio Federal de Inteligencia de Alemania (BND). Estos servicios de inteligencia llevaron a cabo una operación encubierta llamada "Operación Rubicón" desde la década de 1950 hasta 2018, en la que manipularon los dispositivos de cifrados fabricados por Crypto AG para permitir el espionaje de las comunicaciones codificadas por parte de los clientes de la empresa.

Uno de los antecedentes fue en 1992, cuando el ingeniero de ventas, el suizo Hans Bühler, fue detenido en Teherán acusado de espionaje. “Los verdaderos motivos de su detención: los iraníes sospechaban que el servicio secreto estadounidense disponía de una puerta para descifrar los aparatos de Crypto AG”. (Wolff, 2020)

La importancia de fabricar los propios equipos con capacidad de encriptado nos asegura garantizar la seguridad y protección de la información. Al contar con dispositivos fabricados internamente, se puede tener un mayor control sobre los niveles de encriptado aplicados, evitando así potenciales vulnerabilidades que podrían ser aprovechadas por hackers o criminales cibernéticos.

Además, al fabricar los equipos, se tiene la posibilidad de personalizar y adaptar los sistemas de encriptación según las necesidades y requerimientos específicos de la organización.

Otra ventaja, es que se puede garantizar la integridad y autenticidad de los sistemas utilizados. Al tener un mayor control sobre el proceso de fabricación, se puede verificar y asegurar que los equipos no han sido manipulados o alterados antes de su instalación.

Adquirir la capacidad de fabricar nuestros propios medios, como ser equipos de radios, requiere de una ingeniería que en la actualidad el país carece y puede ser desarrollada en un mediano o largo plazo, pero la posibilidad de generar nuestro propio sistema de cripto, que posea los logaritmos necesarios para nuestras fuerzas y además permita que el dispositivo sea adaptable a las facilidades previamente obtenidas en el extranjero. Esta iniciativa presenta la ventaja de reducir los riesgos presentes en la actualidad y la misma puede llevarse a cabo en un corto o mediano plazo.

La segunda acción esta referida a la capacitación de los operadores, donde podemos encontrar que los conocimientos tecnológicos necesarios para poder desempañarse en el rol de combate toman un significado sumamente importante, ya que los mismos le permitirán poder instalar, operar y mantener en forma eficaz y eficiente su grupo de teleinformática.

Poseer el entendimiento sobre los medios provistos, le permite al operador adquirir una capacitación adecuada para explotar todas las facilidades que brinda su grupo y poder solucionar cualquier inconveniente que pueda surgir durante la operación de este.

Dentro de los cursos complementarios, dirigidos al personal de cuadros, no se contempla ninguno que aborde temas de informática, aplicados para poder programar un equipo de radio, configurar centrales telefónicas, router, switch, antenas direccionales y equipos tecnológicos que requieran de una capacitación más técnica y puntual.

En conclusión, la capacitación de los operadores en medidas de seguridad en comunicaciones e informática es de vital importancia para garantizar la seguridad de los sistemas y datos de una organización.

El adiestramiento adecuado les permitirá conocer las principales amenazas y vulnerabilidades existentes en los sistemas de comunicación e informática, así como las técnicas y procedimientos necesarios para prevenir o mitigar los riesgos. Esto incluye la

correcta configuración de los dispositivos, el manejo seguro de contraseñas, la detección de intentos de intrusión y el uso responsable de los recursos tecnológicos.

Además, las directivas sobre medidas de seguridad informática impartidas por la Fuerza contemplan la identificación de los activos críticos de información del sistema, la evaluación de los riesgos asociados, el establecimiento de controles y políticas. En consecuencia, resulta imperativo fortalecer los procedimientos y controles relacionados con la planificación de la seguridad, exigiendo la pronta implementación y la inclusión en las listas de verificación ejecutadas por la Inspectoría General del Ejército, de los parámetros a ser comprobados, con el objetivo de mitigar los peligros a posibles negligencias por parte de los miembros del sistema.

La preparación de los operadores en estas medidas y en el cumplimiento de las políticas establecidas resulta fundamental para asegurar la protección de la información y prevenir posibles incidentes de seguridad que puedan comprometer la integridad, confidencialidad y disponibilidad de los datos.

Aporte Profesional del Autor

Nuestro SCIP, se caracteriza por la interconectividad y redundancia de los medios, que permiten brindan apoyo al sistema de comando y control e inteligencia, pero la concentración de las facilidades no permite la resiliencia necesaria en un teatro de operaciones.

Por tal motivo se propone analizar la factibilidad de modificar el diseño actual, mediante la implementación de un sistema de red de mallas y nodos. La propuesta se fundamenta en la necesidad de optimizar el rendimiento y la eficiencia del diseño, el cual se caracteriza por una estructura centralizada, en la cual los elementos se encuentran concentrados en un único punto.

Ante esta situación, surge la alternativa de adoptar un sistema, el cual implica una distribución más descentralizada de los elementos. De esta manera, se busca mejorar la conectividad y la comunicación entre los diversos puntos de la estructura.

El cambio propuesto se basa en la premisa de que una estructura en red permite una mayor flexibilidad y adaptabilidad a los cambios y demandas operacionales. Además, se espera que esta nueva configuración facilite la detección y corrección de posibles fallos o errores, al no depender de un único punto central de control.

Se plantea llevar a cabo un exhaustivo estudio de factibilidad, el cual englobe aspectos técnicos, económicos y operativos. Será necesario analizar los costos asociados a la implementación de este nuevo sistema, así como los beneficios esperados en términos de eficiencia y rendimiento.

Referencias

Brett, W. (2014). *The Joint Force Commander's Guide to Cyberspace Operations.*

Caballero, F. S. (2003). *Tecnología de la Información y Comunicaciones.* Shpera Pública.

Campos, G. (n.d.). *Inteligencia Estratégica.*

Carl Von Clausewitz. (1832). *Libro VI.*

Easydmarc. (2021). *La Amenaza de los Piratas informáticos – Motivaciones y tácticas: Módulo 2*. https://easydmarc.com/.

Ejército Argentino. (2014). *Medidas de Seguridad de Contrainteligencia.*

Ejército Argentino. (2015). *Conducción para las Fuerzas Terrestres.*

Ejército Argentino. (2016). *Conceptos Básicos sobre Sistemas de Comunicaciones, Informática y Guerra Electrónica de la Fuerza.*

Ejército Argentino. (2022). *Centro de Comunicaciones e Informático de Campaña.*

Ejército Argentino. (2022). *Organización y Funcionamiento de los Estados Mayores.*

Ejército de la República Federativa de Brasil. (2014). *Doutrina Militar de Defesa Cibernética.*

Ejército Español. (2013). *Estrategia de Ciberseguridad Nacional.*

Etienot, N. A. (2014). *Método de gestión de riesgo para el apoyo a la toma de decisiones.*

García, J. N. (2021, mayo 10). *Defensa.com*. https://www.defensa.com/

Gniesko, C. (2017, junio). *Military Review*. https://www.armyupress.army.mil

Joint Publication. (2013). *Cyberspace Operations.*

Lin, H. S. (2010). *Offensive Cyber Operations and the Use of Force.*

López, C. C. (2007). *La Guerra Informática.* Boletín del Centro Naval.

Morales, L. G. (2022). *Evaluación de Riesgo sobre el Sistema.* Instituto de Ciberdefensa de las Fuerzas Armadas.

República Argentina - Poder Ejecutivo Nacional. (2021). *Directiva de política de Defensa Nacional* .

Silva, M. A. (2019, abril). Procedimmiento y Medios para que la Toma de Decisiones sea correcta y oportuna.

Strange, J. (1996). *Understanding Centers of Gravity and Critical Vulnerabilities.*

Strange, J. (2005). *Centers of Gravity & Critical Vulnerabilities.*

Vera, A. (2017). Las Guerras en Red. p. 18.

Vergara, E. d., & Trama, G. A. (2017). *Operaciones Miliatres Cibernéticas.*

Vicenti., C. R. (2014). *Comando y Control en el nivel operacional.* Buenos Aires.

Wolff, J. M. (2020, diciembre 10). *SWI*. https://www.swissinfo.ch

Zarza, L. A. (2016). *Estrategia Militar y su Transfiguración en la era de la Información.*