ESPECIALIZACIÓN EN ESTRATEGIA OPERACIONAL Y PLANEAMIENTO MILITAR CONJUNTO

TRABAJO FINAL INTEGRADOR

TEMA:

La Ciberinteligencia en el Nivel Operacional.

TÍTULO:

Apoyo de la Ciberinteligencia al Teatro de Operaciones.

ALUMNO: MY JORGE ALEJANDRO MAIDANA MUR

TUTOR: CR ERNESTO CLAUDIO BALLOFFET

Resumen

En la República Argentina a partir de la publicación del Libro Blanco de Defensa del año 1998, se establece al ciberespacio como "El quinto espacio" que atraviesa transversalmente los cuatro anteriores (Tierra, mar, aire y espacio). Inicialmente el Ministerio de Defensa y el Estado Mayor Conjunto de las Fuerzas Armadas le dieron relativa importancia a la temática. Hasta que los hechos acaecidos alrededor del orbe en cuanto al uso y la explotación de este "nuevo espacio" por parte de actores de diferente índole, generó la necesidad de atender de manera más urgente el tema.

Tuvieron que pasar casi dos décadas, para que, por una resolución ministerial del año 2014, se creara el Comando Conjunto de Ciberdefensa, desde ese momento a la fecha se presentaron varios proyectos sobre el tema de la Ciberinteligencia en el ámbito Conjunto, pero estos no incluían un elemento de Ciberinteligencia dependiente de este Comando o de la dirección de Inteligencia Conjunta.

El objetivo de este estudio es determinar el mejor diseño para establecer en forma orgánica una Unidad de Ciberinteligencia para brindar apoyo al Comando Conjunto de Ciberdefensa.

Para ello esta investigación se ha apoyado en el estudio de las bases legales vigentes, en las estructuras de Ciberdefensa y Ciberinteligencia de otros estados, para que en base a lo que la ley me permite y los ejemplos, relativos a esta temática, de otras FFAA, llegar a determinar el diseño más eficiente de una organización para apoyar hasta un nivel TO.

La propuesta resultante de este trabajo tiene por finalidad proponer una Unidad con las características y capacidades necesarias para apoyar de una forma eficiente a un comandante de un TO, brindándole la información necesaria, para la mejor explotación del ciberespacio y defensa ante las potenciales amenazas.

definir, en investigaciones posteriores, que clase de material necesitaría la organización para constituir dicho elemento, de acuerdo con las amenazas existentes y aquellas que se aprecie, puedan configurarse en el futuro y que sean de probable empleo por agentes externos y teniendo en cuenta la rapidez con que evolucionan los medios tecnológicos, así como también el conocimiento que debe poseer el personal especializado y que debe ser actualizado sin solución de continuidad, teniendo en cuenta en primer lugar la conformación del elemento y su correspondiente doctrina.

Palabras clave: Ciberespacio, Ciberinteligencia, Ciberactores, Infraestructuras Críticas, Operaciones Militares en el Ciberespacio.

Índice

Introducción

El presente trabajo trata la importancia del apoyo de la ciberinteligencia a las operaciones militares, en particular a nivel Operacional. Experiencias surgidas de diferentes conflictos de años recientes nos dejan experiencias y bondades de su uso por parte de los diferentes actores participantes de los conflictos.

De esas experiencias se desprende la necesidad de conformar un elemento de ciberinteligencia para apoyar al elemento de ciberdefensa a nivel operacional, para dirigir y reunir los esfuerzos de los diferentes componentes.

Problema

Antecedentes y justificación del problema

La Ciberinteligencia se desprende de la explotación del Ciberespacio término que surgió a fines de los años 60´con las primeras redes informáticas, pero que tomó mayor importancia en el corriente siglo con la masificación del uso del internet, hecho que permitió una interconexión a nivel mundial jamás vista. Aparejando el aprovechamiento de este espacio para la obtención de información para su posterior uso, debido a esta masificación del uso del ciberespacio se hizo cada vez más difícil identificar al agresor o agresores, de aquí que no podemos abordar el tema sin conocer la Ciberdefensa y sus diferencias con la misma, cómo también definiciones, grado de actualización e implementación en la materia en el marco mundial y regional.

A nivel mundial, fundamentalmente las potencias, comenzaron su desarrollo en lo respectivo a lo exploratorio, medidas tendientes a la protección y todo tipo de Operaciones inherentes al uso del Ciberespacio.

En materia doctrinaria el (Reglamento de Doctrina Básica para la Acción Militar Conjunta del EMCO (PC 00-01)), entiende que en el sistema de inteligencia militar operacional “debe prevalecer como signo distintivo la creatividad para innovar en la búsqueda permanente de nuevos puntos de vista, nuevas fuentes de información, nuevos medios, procedimientos y técnicas, un sistema de inteligencia creativo es el primer instrumento para evitar la sorpresa, la creatividad en inteligencia es la capacidad de visualizar tempranamente los cambios en el pensamiento enemigo e inferir sus nuevos paradigmas” (Doldán Estrada, 2014). En ese marco, la ciberinteligencia será entendida como el conocimiento resultante del proceso a que es sometida la información resultante de este quinto espacio.

La Ciberinteligencia apoyará a la ciberdefensa contrarrestando los esfuerzos de inteligencia de los ciberactores que busquen afectar negativamente la infraestructura, reputación y personal de la Institución. En la actualidad, la capacidad de desarrollar un esfuerzo de ciberinteligencia, no se encuentra limitada a los Estados, existiendo actores no estatales que constituyen amenazas o riesgos y que cuentan con capacidades de consideración.

El presente trabajo busca determinar cómo debe ser una organización de ciberinteligencia para afrontar las exigencias actuales con respecto a esta área de la conducción, que afrontará el Comando Conjunto de Ciberdefensa, para apoyar de la mejor manera al comandante y a los elementos de Ciber de los tres componentes del Teatro de Operaciones.

Desde 1998, el Ministerio de Defensa ha publicado y actualizado (El libro Blanco de la Defensa Nacional) donde a lo largo de los últimos años incorporó una visión estratégica sobre el "quinto espacio" (el ciberespacio) como ámbito de las operaciones militares, siendo los restantes el Terrestre, Naval, Aéreo y Espacial.

Por su parte, la Ley 25.520/01 de Inteligencia Nacional y sus respectivas reglamentaciones define a la Inteligencia Estratégica Militar como "la parte de la Inteligencia referida al conocimiento de las capacidades y debilidades del potencial militar de los países que interesen desde el punto de vista de la Defensa Nacional, así como el ambiente geográfico de las áreas estratégicas operacionales determinadas por el planeamiento estratégico militar". De este modo, establece que "los organismos de inteligencia de las Fuerzas Armadas tendrán a su cargo la producción de inteligencia estratégica operacional y la inteligencia táctica necesaria para el planeamiento y conducción de operaciones militares".

Considerado desde lo operacional como "operaciones de ciberinteligencia, vigilancia y reconocimiento, que comprenden actividades en el espacio cibernético para reunir inteligencia activa de los sistemas del blanco y del adversario requeridos para apoyar las operaciones militares". Las misiones cibernéticas para la defensa pueden ser apoyadas por las capacidades nacionales o de cada una de las fuerzas armadas. Por su parte, las operaciones cibernéticas de preparación del ambiente operacional son todas las actividades que realizan para preparar y posibilitar la ciberinteligencia, vigilancia y reconocimiento, y las operaciones defensivas y ofensivas. Estas son las operaciones típicas del nivel operacional de guerra.

En cuanto al (PC 21 – 01) es el reglamento que rige el funcionamiento informático dentro de las FFAA, deja dentro de sus proyecciones abierta la necesidad de redactar reglamentos específicos y por cada campo de la conducción referidos a la informatización de las funciones, en este aspecto en el campo de conducción de la Inteligencia tiene la necesidad de constituir la punta de lanza en estos aspectos ya que es quién debe velar por las medidas de seguridad y contrainteligencia en el aspecto informático, tanto como en el físico.

En la actualidad hay presentados proyectos tanto de ciberdefensa como de ciberinteligencia que aún continúan en estudio, pero que en la espera de su aprobación se promulgó el Decreto (571/20 Defensa Nacional) modificando documentos del mismo tipo y directivas, sobre todo del período del año 2015 al 2019, siendo necesario que estos sean objeto de una nueva revisión, modificación y posterior presentación para su aprobación por la superioridad.

De esta forma, se observa una ausencia de reglamentos sobre ciberdefensa y por ende de ciberinteligencia, tanto a nivel conjunto como específico. Esto no demuestra falta de interés o indiferencia, ya que se encuentran en revisión proyectos de reglamentos desde el año 2019 hasta nuestros días.

El tema de investigación propuesto actualmente no es abarcado en la doctrina vigente del ámbito conjunto, no obstante, se presentó durante el 2020 un proyecto de reglamento de Ciberdefensa elevado por El Comando Conjunto de Ciberdefensa al Estado Mayor Conjunto para su aprobación, no así en lo que hace específicamente a la Ciberinteligencia, tanto en el ámbito conjunto cómo en los específicos de las Fuerzas.

En materia doctrinaria de las FFAA vamos a hacer referencia a dos reglamentos a saber: a) (Reglamento de Doctrina Básica para la Acción Militar Conjunta del EMCO (PC 00-01)); b) (Reglamento de Informática para la Acción Militar Conjunta (PC 21-01))

El (PC 00-01) se refiere que, durante la tensión, y de acuerdo a los objetivos que imponga la política, las FFAA junto con otras agencias del Estado desarrollarán una activa inteligencia orientada a evaluar las potenciales amenazas sobre los objetivos de valor estratégico, y producir la inteligencia necesaria que alerte sobre el posible estallido de una crisis. Paralela y progresivamente, se podrán adoptar medidas que contribuyan a disuadir potenciales agresiones y que persuadan acerca de los

costos inaceptables que podrían acarrear tales acciones. Si bien no nombra ni un espacio en particular, el ciber espacio pasa de manera transversal por el resto de los espacios y está presente en todas las infraestructuras críticas de interés nacional.

Por otro lado, conforme a la necesaria anticipación, se podrá establecer la seguridad estratégica. Asimismo, se incrementará la obtención de Inteligencia, y se establecerán los indicios del riesgo de escalada que permitan apreciar la evolución del conflicto. Las conclusiones que de ella se obtengan, servirán principalmente para: contribuir al proceso de toma de decisiones, evitar la sorpresa, y orientar un posible empleo de los medios. Fundamentalmente al cada vez más tecnificados los implementos bélicos y de infraestructura tanto crítica como de uso común, surge la necesidad imperiosa de contar con elementos capacitados para efectuar ciberinteligencia a fin de proveer seguridad y anticipación de potenciales ataques.

La mejor manera de definir la ciberguerra, es decir que es un ciberataque o ciberataques que tienen como objetivo específico la infraestructura civil o gubernamental de un Estado.

Estos ciberataques pueden ser llevados a cabo por un Estado contra otro, pero también por organizaciones terroristas u otros actores no estatales, que suelen estar a sueldo de un país hostil o grupos económicos con intereses sobre las infraestructuras críticas de las Fuerzas Armadas. Es por ello que se hace necesario contar con un elemento especialista en determinar ciertos patrones de ataques o intentos de ataques para prevenir al Comandante al Nivel operacional y que éste a su vez, asesore de manera acertada y precisa al Nivel Estratégico Militar y Nacional.

Formulación del Problema

¿Hasta qué punto es necesario contar con un elemento de Ciberinteligencia a nivel Teatro de Operaciones para optimizar el apoyo al Comando Conjunto de Ciberdefensa?

Objetivos

Como objetivo general del trabajo se busca establecer la misión, funciones y estructura de un elemento para el apoyo de Ciber Inteligencia a nivel Teatro de Operaciones (TO) orgánico del Comando Conjunto de Ciberdefensa; que permita afrontar las necesidades de obtención de información y las medidas de seguridad y

contrainteligencia para las Fuerzas Armadas ante este tipo de ataques, dándole a las mismas una capacidad de la cual carece en la actualidad.

Siendo los objetivos particulares los siguientes:

a. Analizar organizaciones de ciberdefensa y ciberinteligencia de potencias pioneras en la materia, dentro del marco regional y hechos históricos del uso de la ciberinteligencia, para destacar su importancia y extraer experiencias de los mismos a pesar de los muy diferentes marcos legales.

b. Teniendo en cuenta las necesidades y los alcances de una futura organización, determinar la misión general, concepto de empleo y diseño definitivo de la misma y comparar su implementación con el flujo informativo actual.

Metodología a Emplear

La presente investigación se desarrolla sobre la base del método deductivo, con inferencias inductivas; se plantea un objetivo general y Dos objetivos particulares, donde se desarrollan conclusiones parciales para dar respuestas a cada uno de los objetivos particulares, y posteriormente, conclusiones finales que buscan brindar las respuestas al objetivo general planteado. El diseño de la investigación es de carácter explicativo, empleándose como técnica de validación el análisis bibliográfico, documental y lógico.

El trabajo se desarrolla en dos capítulos, el primer tiene por objeto el análisis de las estructuras de ciberdefensa y ciberinteligencia de potencias extracontinentales, dentro del marco regional y hechos históricos de la explotación de la ciberinteligencia, para extraer experiencias de la conducción y explotación de este “quinto espacio” (Libro Blanco de la Defensa Nacional).

Finalmente, el segundo capítulo, se desarrolla en función del análisis de la misión de un elemento de ciberinteligencia a nivel Teatro de operaciones, de manera de determinar la mejor organización para llevar a cabo la misma de manera eficaz y eficiente.

CAPÍTULO 1

Organizaciones de Ciberdefensa y Ciberinteligencia en otros Estados

En el presente capítulo se pretende analizar las organizaciones de ciberdefensa y ciberinteligencia tanto de las potencias pioneras en la temática, como la situación actual dentro del marco regional. También breves ejemplos históricos del uso de ciberinteligencia en conflictos transnacionales, a fin de extraer experiencias y antecedentes de fuerzas que vienen con un desarrollo de más de diez o veinte años en materia de explotación y defensa del espacio cibernético.

Se estructura en tres secciones, abordando inicialmente la estructura de unidades de ciberdefensa y ciberinteligencia de potencias extracontinentales a saber: a) Reino de España; b) Estados Unidos de Norteamérica; c) Reino Unido de Gran Bretaña e Irlanda del Norte; d) Federación Rusa. En una segunda sección, se analiza las organizaciones de ciberdefensa y ciberinteligencia dentro del marco regional con los siguientes países a saber: a) República federativa del Brasil; b) República de Chile; c) República de Colombia. La tercera sección, pretende abordar ejemplos históricos del uso del espacio cibernético en diferentes conflictos.

SECCIÓN I

Organizaciones de Ciberdefensa en potencias pioneras en la materia

REINO DE ESPAÑA

El organismo de ciberdefensa de dicho estado es el denominado Mando Conjunto Del Ciberespacio (MCCD) Subordinado al Jefe de Estado Mayor de la Defensa (JEMAD), responsable del planeamiento y la ejecución de las acciones relativas a la ciberdefensa en las redes y sistemas de información y telecomunicaciones del Ministerio de Defensa u otras que pudiera tener encomendadas, así como contribuir a dar la respuesta adecuada en el ciberespacio ante amenazas o agresiones que puedan afectar a la Defensa Nacional. La creación del MCCD es el resultado de un proceso gradual en el que se destacan cinco hitos: a) 28 de enero de 2011, aprobación por el JEMAD de la Visión de la Ciberdefensa Militar; b) 28 de Julio de 2011, aprobación por el JEMAD del Concepto de Ciberdefensa Militar; c) 12 de Julio de 2012, aprobación por el JEMAD del Plan de Acción para la Obtención de la Capacidad de Ciberdefensa Militar; d) 19 de Febrero de 2013, el Ministro de Defensa promulga la Orden Ministerial 10/2013, por la que se crea el Mando Conjunto de Ciberdefensa; e) 19 de Mayo de 2020, el Consejo de Ministros aprobó un Real Decreto que introduce modificaciones en la estructura de las FFAA: refuerzo del EMACON y la creación del MCCD (Ciberespacio).

Teniendo como objetivos generales garantizar la disponibilidad, integridad y confidencialidad de la información, así como la integridad y disponibilidad de las redes y sistemas que la manejan y tenga encomendados, además, Obtener, analizar y explotar la información sobre ciberataques e incidentes en las redes y sistemas de su responsabilidad, esto se traduciría en ciberinteligencia para nuestra doctrina. Otras tareas son, ejercer la respuesta oportuna, legítima y proporcionada en el ciberespacio ante amenazas o agresiones que puedan afectar a la Defensa Nacional y; además; definir, dirigir y coordinar la concienciación, la formación y el adiestramiento especializado en materia de ciberdefensa.

Siendo su ámbito de actuación las redes y sistemas de información y telecomunicaciones de las FFAA, así como aquellas otras redes y sistemas que específicamente se le encomienden y que afecten a la Defensa Nacional. Se presentan dos áreas de Operaciones de Ciberdefensa: a) Área Fija: redes y sistemas de TICs que se utilizan del Ministerio de Defensa en territorio nacional o en el despliegue de las Fuerzas Armadas en el exterior; b) Área Variable: parte del Ciberespacio de interés militar necesario para desarrollar una operación militar específica o responder a amenazas o agresiones que puedan afectar a la Defensa Nacional.

Con respecto a la estructura orgánica cuenta con la jefatura propiamente dicha, una secretaria y el Estado Mayor. La Jefatura de Operaciones es el órgano responsable de la ejecución de las operaciones de Ciberdefensa a través de las acciones de defensa, explotación y respuesta en el ciberespacio, coordinando las actividades de los Centros de Operaciones de Seguridad (COS) del Ministerio de defensa, tanto permanentes como desplegables, cuenta con cuatro grupos a saber: a) Grupo de Defensa ejecuta actividades orientadas a la protección frente a cualquier acción que comprometa los sistemas de información y telecomunicaciones y la información que manejan, así como, cuando proceda, a su recuperación; b) Grupo de Explotación ejecuta acciones orientadas al conocimiento de las capacidades de actuación en el ciberespacio de potenciales adversarios y agentes hostiles; c) Grupo de Respuesta ejecuta acciones de respuesta en el ciberespacio ante amenazas o ataques; d) Grupo Técnico: apoyo técnico (asesoramiento técnico, evaluación de productos y la simulación y el desarrollo de software).

Además, posee una Jefatura de Administración y Servicios (JAS) que es el órgano responsable de prestar el apoyo administrativo, técnico y seguridad de los sistemas de información y telecomunicaciones.

Como medios para la ejecución de estas actividades podemos destacar tres sistemas, el primero la plataforma CYBER RANGE (Es una plataforma virtual que permite simular

entornos operativos reales –estáticos o desplegables, clasificados o no clasificados– para la formación y el entrenamiento –individual o colectivo– de profesionales, así como la experimentación, el testeo y la validación de nuevos conceptos, tecnologías) que posee dos capacidades destacables una es de ejecutar ejercicios de ciberdefensa, produciendo ciberataques en entornos seguros, lo cual da paso a su segunda capacidad y facilidad que es la formación de hacking ético y análisis forense para militares españoles. Luego cuentan con la plataforma HONEYPOT (Es un sistema informático que se "sacrifica" para atraer ciberataques, como un señuelo. Simula ser un objetivo para los hackers y utiliza sus intentos de intrusión para obtener información sobre los cibercriminales y la forma en que operan o para distraerlos de otros objetivos) que es un software o grupo de ordenadores cuyo objetivo es atraer a potenciales atacantes, simulando ser sistemas vulnerables o débiles a los ataques. Es una herramienta de seguridad informática utilizada para recoger información sobre los atacantes y sus técnicas. Para finalizar cuentan con el RiskPAC (Es un sistema automático de evaluación de riesgos) el mismo es un paquete elaborado en EEUU por la compañía CSCI (Computer Security Consultants Inc.) y está orientado a la realización de análisis de riesgos y la definición de la influencia de este riesgo en los procesos, como cualitativo de los riesgos.

ESTADOS UNIDOS DE NORTEAMÉRICA

El Cibercomando de Estados Unidos, también conocido por las siglas USCC (del inglés United States Cyber Command), es un Comando Unificado de las Fuerzas Armadas de Estados Unidos bajo el mando del Departamento De Defensa De Los Estados Unidos. Fue creado el 23 de junio de 2009. Su misión es el uso de técnicas informáticas con el objetivo de velar por los intereses de Estados Unidos o sus aliados. Esto incluye la protección directa de sistemas informáticos, actuaciones de respuesta rápida frente a ataques o incluso ejecutar ataques para proteger sus intereses. El Cibercomando trabaja en estrecha colaboración con la NSA (Agencia Nacional de Seguridad). Desde su fundación el director del Cibercomando ha sido a la vez director de la NSA.

USCYBERCOM tiene como misión centralizar el comando de las operaciones ciberespaciales, fortalecer las capacidades ciberespaciales del Departamento de Defensa, e integrar y reforzar la ciberpericia del Departamento de Defensa. Consecuentemente, USCYBERCOM mejorará las capacidades del Departamento de Defensa para garantizar información y redes de comunicación fiable y resistente, contrarrestar las amenazas ciberespaciales y garantizar acceso al ciberespacio. Los esfuerzos del USCYBERCOM también apoyarán las habilidades de los Servicios Armados para gestionar con confianza

operaciones de alto ritmo en forma efectiva, además de proteger sistemas de control y comando y la infraestructura ciberespacial en la que se basan las plataformas de sistemas de armas de interrupciones, intrusiones y ataques.

Para conducir el poder cibernético, el USCYBERCOM lidera una fuerza de misión cibernética de 133 equipos en todo el Ejército, La Marina, La Fuerza Aérea y el Cuerpo De Marines. Esta fuerza incluye 13 equipos misioneros (Referido a misiones de ciberinteligencia) nacionales para defenderse de las amenazas cibernéticas más importantes para la nación; 68 equipos de protección cibernética para defender las redes y sistemas contra amenazas; 27 equipos de misiones de combate para realizar ataques integrados en el ciberespacio; y 25 equipos de soporte cibernético para proporcionar soporte analítico y de planificación.

Con respecto al marco legal, sólo se remarcará un aspecto particular por su relevancia otorgada a la temática especifica, ya que al existir diferencias abismales con nuestra legislación los demás aspectos carecen de relevancia para este trabajo. La Estrategia Nacional de Inteligencia de 2019: identifica la inteligencia cibernética como uno de los cuatro objetivos de misión de la Comunidad de Inteligencia (junto con el antiterrorismo y contra proliferación) y el Departamento de Seguridad Nacional de EE. UU. (DHS) ha identificado Analistas de amenazas ciber/ analistas de contrainteligencia ciber como uno de varios trabajos y tareas de misión crítica.

REINO UNIDO DE GRAN BRETAÑA E IRLANDA DEL NORTE

Para entender la organización particular de este Estado es menester comenzar por la estructura de las responsabilidades cibernéticas a nivel Nacional, en primer lugar, nombrar a la Oficina Central de Comunicaciones del Gobierno (GCHQ)**,** es una de las tres principales agencias de inteligencia, junto al MI5 y MI6. Es una organización gubernamental de seguridad e inteligencia, creada para proporcionar inteligencia de señales y seguridad de la información al Gobierno británico y a sus FFAA, con dependencia directa del Secretario de Asuntos Exteriores y Commonwealth.

En 2016, bajo la órbita de la GCHQ, se creó el Centro Nacional de Seguridad Cibernética, con sede en LONDRES, como proveedor de asesoramiento y apoyo al sector público y privado sobre cómo evitar y contrarrestar las amenazas cibernéticas, absorbiendo y remplazando al CESG, al Centro de Evaluación Cibernética (CCA, Centre for Cyber Assessment), el Equipo de Respuesta a Emergencias Informáticas del REINO UNIDO (CERT UK, Computer Emergency Response Team UK) y a las responsabilidades en materia de

cibernética del Centro de Protección de Infraestructura Nacional (CPNI, Centre for the Protection of National Infrastructure).

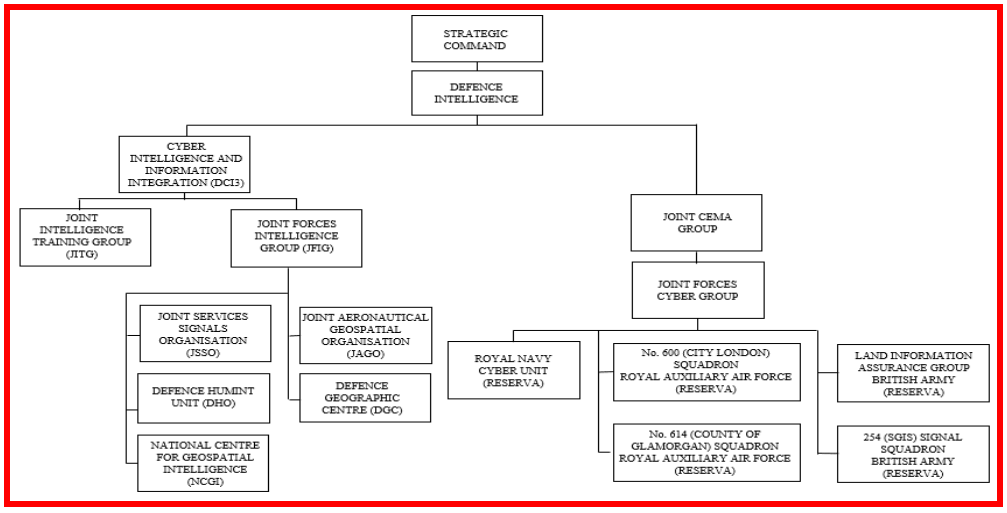


Gráfico 1(Sistema Ciber del RUGBIN)

El Comando Estratégico (Strategic Command), administra las capacidades conjuntas asignadas de las tres Fuerzas. En 2012, asumió la responsabilidad de las operaciones conjuntas, inteligencia, servicios médicos, sistemas de información, capacitación y educación, fuerzas especiales y bases en el extranjero. Lidera el dominio cibernético.

El Jefe de Inteligencia de Defensa (DI, Defence Intelligence), órgano conjunto, es el principal asesor en temas de Inteligencia Militar Estratégica. Proporciona inteligencia y asesoramiento para asistir a las decisiones de política, despliegue e investigación, trabajando junto con otros Departamentos gubernamentales, la UE y la OTAN.

El Director de Ciber Inteligencia e Integración de la Información (DCI3, Director of Cyber Intelligence and Information Integration) es responsable de la provisión de servicios especializados de inteligencia, imágenes y soporte geográfico y de la capacitación en inteligencia y seguridad de las FFAA.

El Grupo de Actividades Cibernéticas y Electromagnéticas Conjunto (JCEMAG, Joint Cyber and Electromagnetic Activities Group): fue diseñado para coordinar actividades cibernéticas y electromagnéticas (CEMA) a nivel operativo, permitir actividades de apoyo y producir una estrategia para optimizar la aplicación de las capacidades de dicha naturaleza.

El Grupo Cibernético de Fuerzas Conjuntas (JFCyG, Joint Forces Cyber Group), planifica y coordina las operaciones de guerra cibernética. Además, cuenta con la Unidad Cibernética Conjunta (Reserva) que se estableció en respuesta a una creciente amenaza de guerra cibernética y para permitir que los militares se beneficien de la experiencia de especialistas civiles en Tecnologías de Información. El Ministerio de Defensa reclutó

reservistas como expertos en informática para trabajar junto a las fuerzas regulares en la creación de la nueva Unidad. Su rol principal es proteger las redes de computadoras y salvaguardar los datos vitales puede efectuar ataques en el ciberespacio. Inicialmente, el reclutamiento de reservistas se centró en el personal regular que abandonó las FFAA, reservistas actuales y anteriores, con las habilidades requeridas y civiles con las habilidades y conocimientos tecnológicos apropiados. Las siguientes unidades aportan personal al JFCyG: a) Unidad Cibernética de Reserva - Marina Real; b) Escuadrón No. 600 - Real Fuerza Aérea Auxiliar; c) Escuadrón No. 614 - Real Fuerza Aérea Auxiliar; d) Grupo de Aseguramiento de Información Terrestre - Reserva del Ejército; e) Escuadrón de Señales 254 - Reserva del Ejército.

En cuanto al nivel del Instrumento Militar Terrestre el 31 de julio de 2019, el Ejército británico anunció la creación de la 6ta División**,** una nueva División de Guerra Cibernética para centrarse en las amenazas digitales, en respuesta a las amenazas de Estados hostiles y grupos extremistas. La nueva Unidad se concentrará en la guerra cibernética, la propaganda, la inteligencia y la vigilancia. A tal efecto, sus elementos conformantes provendrán de Unidades existentes dentro del Ejército, así como de un pequeño número de efectivos de la Marina Real y la Real Fuerza Aérea. Esta División comprende capacidades de inteligencia, contrainteligencia, guerra cibernética, electrónica, operaciones de información y guerra no convencional. Cabe destacar que la 6ta División no sólo desarrollará operaciones de guerra cibernética defensiva sino también actividades cibernéticas ofensivas y operaciones de información para contrarrestar actividades y amenazas de esta naturaleza de otros Estados, de esta manera, está conformada por: a) La Brigada de Señales 1; b) La Brigada de Señales 11; c) La Brigada de ISR 1; d) La Brigada 77.

La Brigada 77 se creó en enero de 2015, en el marco de una restructuración de unidades militares, que incluyó al 15 Grupo de Operaciones Psicológicas y el Grupo de Operaciones de Medios. En ese momento, funcionarios revelaron que se usarían las redes sociales, como Facebook y Twitter, para “luchar en la era de la información”. En ese sentido, el sitio web del Ejército detalla que las misiones de la Brigada 77 incluyen “planificar la actividad de información”, “análisis de adversarios y audiencia” y “recopilar, crear y difundir contenido de medios digitales en apoyo de tareas designadas”, entre otras.

FEDERACIÓN RUSA

En el año 2000, en relación con la seguridad informática, la doctrina militar determinó la utilización de los servicios de seguridad e inteligencia para combatir los ataques que se presenten en este ámbito, siendo el Departamento Central de Inteligencia (en ruso, Главное Разведывательное Управление, Glávnoye Razvédyvatelnoye Upravlenie, o GRU) el organismo competente en la materia.

Dentro de su estructura, se encuentra el Servicio de Inteligencia Extranjera y el Servicio Federal de Seguridad, que lleva cabo operaciones de control interno y contrainteligencia. Además de la actividad mencionada precedentemente (seguridad informática), es responsable de la inteligencia militar en el exterior, la cual obtiene de los Agregados Militares, así como también por medio de informantes que incorpora al efecto. No posee competencia para espionaje interno, son las Secciones de Inteligencia pertenecientes a las Unidades Militares desplegadas en el territorio nacional las que se ocupan del mismo. Se destaca la dependencia de las Secciones al GRU y la de éste al Estado Mayor General.

Se destacan las siguientes capacidades del GRU: SIGINT (inteligencia de señales), HUMINT (inteligencia humana), OSINT (inteligencia de fuentes abiertas), GEOINT (inteligencia geoespacial), MASINT (inteligencia de medición) y TECHINT (inteligencia técnica).

El GRU está organizado en trece directorios principales, más ocho directorios, secciones y servicios auxiliares. El directorio competente en la materia de ciberseguridad es el sexto que se encarga de dirigir las Radio divisiones de Propósito Especial y, en general, toda la inteligencia de señales.

Como hito más importante y reciente en cuanto al marco legal de este Estado se destaca que en abril de 2019, se aprobó la Ley (*RUNET)*, ley de internet soberana, que entró en vigor en noviembre de 2019, por medio de la cual RUSIA estableció el desarrollo de un servidor de internet propio, además de que por ley desde el 2017 las industrias que son críticas para la economía nacional son consideradas como prioridad ante ataques cibernéticos y protegidas por elementos pertenecientes al GRU.

SECCIÓN II

Organizaciones de Ciberdefensa dentro del marco regional

REPUBLICA FEDERATIVA DEL BRASIL

La Presidencia de la República, cuenta con el apoyo del Gabinete de Seguridad Institucional (GSI) para avanzar con la implementación de medidas referidas a la Seguridad Cibernética y tiene bajo su órbita la Agencia Brasileña de Inteligencia (ABIN); además, la Secretaría Especial de Asuntos Estratégicos, dependiente de la Secretaría General, asesora al Presidente respecto a dicha temática. El Ministerio de Defensa (MD) y el Estado Mayor Conjunto de las FFAA, tienen la responsabilidad por desarrollar el Programa "Defensa Cibernética en la Defensa Nacional", que conjuntamente realizan con el Ejército Brasileño, que tiene bajo su responsabilidad el desarrollo de la Ciberdefensa, no solo para la Fuerza Terrestre, sino para todo el Gobierno Federal.

El Comando de Defensa Cibernética del Ejército (ComDCiber), es el Órgano Central del Sistema de Defensa Cibernética del Ejército, responsable por coordinar e integrar las actividades del sector; proporcionar al Ministerio de Defensa y las FFAA los medios necesarios para ejercer la defensa y el control continuo del espacio cibernético de interés; garantizar un flujo ágil y seguro de información confiable y oportuna; e impactar positivamente las áreas científicas, tecnológicas e industriales del país. Bajo su dependencia, la Escuela Nacional de Defensa Cibernética (EsNaDCiber) y el Centro de Defensa Cibernética.

El Centro de Defensa Cibernética (CDCiber – BRASILIA/DF) es el Componente Operacional de Defensa y Guerra Cibernética, para mejorar la estructura y seguridad de la red virtual, entrenar y capacitar a los efectivos militares, desarrollar herramientas (Simulador de Operaciones Cibernéticas - SIMOC), e investigar en Inteligencia y Seguridad Cibernética, Criptografía, entre otros. Junto con las otras FFAA son las responsables por la Guerra Cibernética.

SISTEMA BRASILEÑO DE DEFENSA CIBERNÉTICA		
Nivel	**Jurisdicción**	**Órganos Ejecutores**
Nacional	**Seguridad de la Información y Seguridad Cibernética**	**. Gabinete de Seguridad Institucional** (GSI) **. Agencia Brasileña de Inteligencia** (ABIN)
Estratégico	**Defensa Cibernética**	**. Ministerio de Defensa** (MD) **. Estado Mayor Conjunto de las FFAA** . Fuerzas Armadas
Operacional	**Guerra Cibernética** (**Inteligencia**, Ciencia y Tecnología, Operaciones, Doctrina y RRHH)	**Comando de Defensa Cibernética** del Ejército Brasileño (con participación de la Armada y de la Fuerza Aérea)
Táctico		**Centro de Defensa Cibernética**

Gráfico 2 (Sistema Ciber brasileño)

El Centro de Defensa Cibernética (CDCiber – BRASILIA/DF) es el Componente Operacional de Defensa y Guerra Cibernética, para mejorar la estructura y seguridad de la red virtual, entrenar y capacitar a los efectivos militares, desarrollar herramientas (Simulador de Operaciones Cibernéticas - SIMOC), e investigar en Inteligencia y Seguridad Cibernética, Criptografía, entre otros. Junto con las otras FFAA son los responsables por la Guerra Cibernética.

Para resaltar ciertos aspectos del marco legal en 2012, se actualizó la Política de Defensa Cibernética, entre los objetivos que plantea incorpora la inteligencia cibernética que tiene por misión colaborar con la producción de conocimiento de inteligencia, desde la fuente cibernética, de interés para el Sistema de Inteligencia de Defensa (SINDE) y los organismos gubernamentales involucrados con Seguridad de la Información y las Comunicaciones (SIC) y Ciberseguridad, especialmente la Oficina de Seguridad Institucional de la Presidencia de la República. Asimismo, este objetivo presenta ciertas pautas generales: a) Adaptar la doctrina

de la inteligencia para insertar la fuente cibernética en el contexto de la integración de fuentes de datos con el objetivo de producir conocimiento; b) Crear estructuras de Ciberinteligencia, de acuerdo con las necesidades de las agencias centrales de inteligencia de la FFAA y del Sistema Militar de Defesa Cibernética (SMDC), para aplicar métodos científicos y sistemáticos, buscando extraer y analizar datos de la fuente cibernética, produciendo conocimiento de interés; c) Establecer un canal sistémico / técnico entre el cuerpo central del SMDC y los órganos centrales de Inteligencia de la FFAA, dentro del alcance de SINDE, con respecto al sector cibernético; d) Examinar las infraestructuras de información crítica asociadas con amenazas internas y externas, reales o potenciales, para contribuir a la formación de la conciencia situacional necesaria para las actividades de inteligencia.

En cuanto a los materiales el Estado busca llevar adelante desarrollos tecnológicos propios, de origen nacional, mediante asociaciones Público-Privadas, con Empresas del Sector propias de BRASIL. Así quiere evitar la dependencia tecnológica de países extranjeros y además, limitar la injerencia externa en la materia, que pueda derivar en vulnerabilidades que permitan la intromisión y exposición de los datos, infraestructuras críticas y sistemas de comunicación.

El Centro de Instrucción de Guerra Electrónica (CIGE) del Ejército junto con las Empresas Brasileñas DECATRON y RUSTCON (Es una empresa brasileña que promueve el desarrollo de herramientas y soluciones modernas para la defensa de los intereses nacionales brasileños, incluida la infraestructura crítica) desarrollaron el Simulador de Operaciones Cibernéticas (SIMOC). Además, la Empresa nacional BLUEPEX (empresa del Estado para soluciones cibernéticas en negocios) participó de la creación del Antivirus DEFESA.BR. Además, la Asociación de las Empresas Brasileñas de Seguridad de la Información - Regional de SAN PABLO (ASSESPRO-SP) junto con el Instituto de Inteligencia Cibernética han creado el Comité de Inteligencia Cibernética, siendo este un órgano dedicado a las cuestiones público-privadas relacionadas a la Seguridad, accesibilidad, educación y difusión de los conocimientos referidos específicamente a la Ciberinteligencia.

La estrategia cibernética del Brasil contribuye a obtener la autonomía y reducir la dependencia en el desarrollo de productos cibernéticos de origen nacional, al mismo tiempo que, coopera con otros países a fin de estar preparado para detectar y contrarrestar los ataques que pueden afectar a otros países, compartiendo y recibiendo información sobre las amenazas detectadas.

REPUBLICA DE CHILE

Actualmente el Sistema de Inteligencia del Estado (SIE) está compuesto por organizaciones correspondientes al MINISTERIO DE DEFENSA que nuclea por medio del Estado Mayor Conjunto a las Direcciones de Inteligencia de las tres Fuerzas Armadas, y otra correspondiente al MINISTERIO DEL INTERIOR, que nuclea a la Agencia Nacional de Inteligencia (ANI), la Dirección de Inteligencia de Carabineros y la Jefatura Nacional de Inteligencia Policial. Todos los órganos de inteligencia coordinan su labor por medio de un Comité de Inteligencia.

El 09 de noviembre de 2017, el Gobierno aprobó la Política Nacional de Ciberseguridad 2017-2022 (PNCS), constituyéndose en el primer instrumento de política pública del Estado tendiente a desarrollar una estrategia nacional en materia de ciberdefensa. Dicha Política impulsó al Ministerio de Defensa a formular políticas específicas, que contemplen las definiciones en torno a cómo serán protegidas estas redes y cómo las capacidades de la Defensa Nacional pueden colaborar en la formación de un ciberespacio libre, abierto y seguro.

El 30 de octubre de 2019, luego de varios días de crisis social, comienza a ser analizado el Sistema De Inteligencia Del Estado (SIE) y se establece un Programa para modificar tal Sistema, ya que fue verificada la imposibilidad de adelantarse a los hechos ocurridos, crítica principal que recibió la ANI.

El 06 de noviembre de 2019, el Presidente, Sebastián Piñera, aprobó una directiva para el periodo 2019-2022, buscando coordinar a todo el sistema de las FFAA y las de Orden y Seguridad del Estado.

El proyecto de Ley pendiente de aprobación basado en la directiva antes mencionada, decidió separar las competencias propias de la Ciberdefensa, dejándolas en manos del Ministerio De Defensa; Ciberseguridad, que pasan a ser asumidas por el Ministerio del Interior; y Ciberinteligencia, definidas desde la óptica de la ANI, coordinadas a través del Comité Interministerial de Ciberseguridad.

El Proyecto de Ley también busca consolidar el desarrollo de la Ciberinteligencia, “mejorando la obtención de información, procesamiento y producción de Inteligencia, mediante la explotación de fuentes contenidas en el ciberespacio”. Respecto de la actividad de Ciberinteligencia, no existe en la actualidad un departamento exclusivo que realice la actividad.

En la modificación en proceso la ANI pasará a ocupar un papel predominante como cabeza del SIE, y dentro de su División de Contrainteligencia se creará un Departamento de

ciberdefensa, que por medio del Comité de Inteligencia nucleará los esfuerzos de la Dirección de Inteligencia del EMCO y de las Policías, a los cuales se sumarán las Direcciones de inteligencia, Gendarmería y Servicio Nacional de Aduana (estas últimas, a crearse).

El 14 de enero de 2020, la Comisión de Hacienda del Senado aprobó las normas específicas del Proyecto de Ley que moderniza el SIE y de la ANI.

El 15 de mayo 2020, el Presidente otorgó de "suma urgencia" el tratamiento final del Proyecto de ley que busca fortalecer y modernizar el Sistema de Inteligencia del Estado (SIE) conformado -entre otros- por la ANI y representantes de las Fuerzas Armadas, Carabineros y Policía de Investigaciones (PDI).

REPUBLICA DE COLOMBIA

La Seguridad Digital de COLOMBIA está a cargo del Ministerio de Defensa, a través del Grupo de Respuesta a Emergencias Cibernéticas (ColCERT), el Comando Conjunto Cibernético de las Fuerzas Militares (CCOC) y el Centro Cibernético Policial (CCP). El Ministerio de Defensa articula y lleva a cabo las políticas de Seguridad Digital de Colombia, si bien los esfuerzos son intersectoriales y en cooperación con entidades públicas y privadas, la cúpula del Ministerio de Defensa abarca tanto los esfuerzos de Ciberseguridad como los de Ciberdefensa.

El CCOC planea, coordina, integra y conduce operaciones militares (de defensa, inteligencia y respuesta) en el ciberespacio para la defensa de los intereses nacionales y de la infraestructura crítica cibernética nacional.

También se realiza ciberinteligencia, la cual está contenida dentro de las políticas de Ciberdefensa del Ministerio de Defensa, ejemplo de esto es la Operación "BASTÓN" del Ejército Nacional, dicha Operación contempla actividades de inteligencia y contrainteligencia, para evitar que efectivos vulneren las MSCI y para obtener información de integrantes de los Grupos Armados Organizados (GAO) y Bandas Criminales (BACRIM).

Las Unidades Cibernéticas de las Fuerzas Militares de Colombia tratan al ciberespacio como un ámbito estratégico, operacional y táctico. Se organizan, entrenan y equipan a fin de aplicar medidas de prevención, disuasión, contención, protección y reacción, que permitan fortalecer las capacidades de Ciberdefensa, para enfrentar las amenazas o incidentes informáticos, que puedan afectar a la Fuerza, a la infraestructura crítica del país o poner en riesgo la Seguridad Nacional.

Al ser una actividad relativamente reciente, todavía continúan en desarrollo las capacidades. El CCOC pasó de gestionar aproximadamente cinco mil incidentes cibernéticos,

en todo el año 2018, a seis mil doscientos, en lo que va del año 2021, por lo que se espera que, para el año 2022, estas capacidades aumenten a aproximadamente siete mil quinientos incidentes gestionados.

El estado genera convenios con corporaciones informáticas y con países con experiencia en el ciberespacio, actualmente el CCOC tiene un convenio con ORACLE (empresa de soluciones Tecnológicas) para la producción de software. A su vez, se intercambia conocimientos con Estados Unidos, Letonia y la OTAN.

Se conoce que se ha licitado en al menos dos ocasiones la compra de notebooks y software de forensia cibernética (aplicación de técnicas de investigación y análisis informático para determinar una evidencia) para sus Unidades de Inteligencia. Tanto el Batallón de Ciberinteligencia (BACIB) como el Batallón de Contrainteligencia de Seguridad de la Información (BACSI) utilizan software como PERSEO para monitoreo de celulares que utilizan el Sistema Operativo Android.

En el año 2019, el Ejército Nacional adquirió el Software "HOMBRE INVISIBLE" de la empresa española MOLLITIAM INDUSTRIES (Es una compañía que integra experiencia y capacidades propias en las áreas de desarrollo de soluciones y tecnología software con sede en España), este software tiene la particularidad de penetrar cualquier dispositivo conectado a internet, pudiendo obtener la información almacenada en este sin dejar rastro alguno.

Los siguientes sistemas son los que se conoce que utilizan las fuerzas colombianas relacionadas con el ámbito de la ciberdefensa; LÉGOLAS permite generar un hipervínculo, el cual realiza un reconocimiento pasivo de la máquina del objetivo; PANZER es una herramienta de intrusión informática, ingresa a computadoras e inclusive enviar archivos a los sistemas informáticos del adversario; OSIRIS se trata de un software de monitoreo de redes internas, cambios en el sistema de archivos de computadoras, también es capaz de monitorear listas de usuarios, listas de grupos y extensiones; CERBERUS consta de un troyano para celulares con Sistema Operativo Android que permite al atacante controlar el dispositivo de forma total y remota.

SECCIÓN III

Experiencias, Antecedentes y Casos de uso de Ciberinteligencia

Red October 2007 Patrullaje cibernético

Su objetivo era recopilar información de inteligencia de organismos gubernamentales, diplomáticos y militares. Consistió en un software malicioso que enviaba data activamente a múltiples servidores (data center), que pueden manejar de manera remota las computadoras afectadas por el malware (Es el resultado de la unión de las palabras malicious software o software malicioso). No tenía como blanco cualquier computadora, sino que atacaba selectivamente a objetivos geopolíticos, como agencias de gobierno, embajadas, centros de investigación nuclear y bases militares. El principal objetivo era obtener documentos clasificados de organizaciones, incluida información de inteligencia geopolítica, credenciales para acceder a sistemas clasificados de computación y datos de aparatos móviles y equipo de red personal, informó Kaspersky (Empresa conocida por ser proveedor de antivirus y desarrolladora de software).

La forma de infección era a través de un plug-in que se instalaba en Adobe Reader o Microsoft Office, y seguía funcionando a pesar de que el usuario lo desinstalara. Si bien estaba preparado para atacar computadoras, también podrían estar en riesgo smartphones y tablets. Los investigadores indican que el ataque comenzó al menos desde 2007 y los principales objetivos fueron países de Europa del Este, pero hubo reportes de incidencias desde América Del Norte y Europa Occidental.

Georgia 2008 Identificación de ciberamenzas

Los ciberataques se llevaron a cabo en agosto de 2008 y bloquearon el acceso a sitios del gobierno, de bancos y de la prensa de Georgia. El incidente ocurrió justo cuando las tropas rusas salían en defensa de Osetia Del Sur (Estado de la zona del Cáucaso ruso), cuya capital fue dejada en ruinas por un ataque lanzado por Georgia en un conflicto armado que duró aproximadamente una semana.

Los investigadores norteamericanos afirman que la totalidad del frente de ciberataques estaba compuesto por civiles, algunos lo hacían involuntariamente al formar parte de “redes zombis”, pero otros habían sido reclutados en sitios de Internet, incluyendo redes sociales estadounidenses, para cooperar en el ataque de forma voluntaria. “Muchos de los ciberataques y operaciones militares se lanzaron con tan poco tiempo de diferencia que tuvo que haber una cooperación cercana entre los militares rusos y los atacantes virtuales civiles”, dice parte del

informe. Asimismo, la US-CCU (Organización norteamericana que publica documentos de ciberseguridad) sospecha que todo el proceso de preparación de los ataques, como registrar nombres de dominio y establecer sitios nuevos, se había realizado con anticipación, y los atacantes virtuales sólo debían esperar una señal para comenzar. De esta manera se observa la facilidad dentro de este espacio de deslindarse de responsabilidades por parte de los reales organizadores o cerebros de las operaciones ejecutadas.

Buckshot Yankee 2008 Determinación de tácticas, procedimientos y técnicas de empleo

Unas de las brechas más importantes, en el sistema de ordenadores militares de Estados Unidos de Norteamérica, la produjo en 2008 una agencia de inteligencia extranjera que consiguió insertar un código malicioso en un ordenador portátil militar norteamericano, emplazado en Oriente Medio, que estaba conectado a una red dirigida por el Comando Central de las FFAA estadounidenses. El código se extendió sin ser detectado y estableció una cabeza de puente digital que transfería datos a servidores de otro país. En este caso a pesar de toda la tecnología de forensia cibernética puesta a disposición para llegar al origen de la agresión, solamente terminaron en conjeturas de los probables responsables.

Estonia Blockchain, Forensia Informática

En 2007 Estonia sufrió un ciberataque cuando un grupo de piratas informáticos de Rusia dejaron en negro las webs del Gobierno. El episodio, más que asustarlos y paralizarlos, los llevó a crear proyectos de seguridad para monitorear constantemente sus sistemas informáticos, apoyando sus bases de datos bajo la tecnología Blockchain (se puede definir como una estructura matemática para almacenar datos de una manera que es casi imposible de falsificar). Este sistema de criptografía y algoritmos para verificar las transacciones, y así seguir la pista de cualquier intercambio que lleve valor, incluida información, está tecnología es la misma base de la existencia de las criptomonedas tales como Bitcoin, Ethereum y otros desarrollos basados en estas Blockchain. Esta tecnología se basa en algoritmos de autenticación que hasta el momento demostraron ser las más seguras dentro de los datos que se encuentran en el ciberespacio. En lo que se refiere a la forensia informática, se trata de un filtrado de archivos de determinados programas buscando ciertas anomalías, una vez aislados estas extensiones o archivos anómalos se los debe someter a más filtros para determinar si fehacientemente son maliciosos o sólo errores de programación.

Conclusiones Parciales

En cuanto a los Sistemas de Ciberdefensa y Ciberinteligencia de las potencias extracontinentales pioneras, podemos destacar todas las funciones de defensa y explotación que nuestro marco legal permite, en el caso particular del Reino de España algunos de los sistemas utilizados son perfectamente compatibles con las responsabilidades y misiones que le puedan caber en el ámbito de la Defensa aplicado a nuestro país, particularmente este tipo de organización facilita mucho el trabajo de un Comando Conjunto.

Del Reino Unido de Gran Bretaña podemos extraer la división de los diferentes niveles de la conducción y el uso de materiales y equipos dentro del Nivel Operacional y Nivel Táctico, inclusive conociendo las unidades destinadas dentro de cada Nivel.

De las potencias tales como Estados Unidos de Norteamérica y la Federación Rusa, vale destacar desde la época que vienen desarrollando sus sistemas de ciber patrullaje y ciberataque, para conocer los sistemas, eventualmente adquirirlos o emularlos en el centro de desarrollo de software de nuestro país, ya sea en los centros de software en el ámbito civil o de cada una de las Fuerzas Armadas.

Ya adentrado en el marco regional cabe destacar no sólo la infraestructura y el desarrollo de la temática en la República Federativa del Brasil, sino la intención del desarrollo de software manifiesto desde la creación de sus entes de ciberdefensa. Es importante por el marco de colaboración mutua que existe entre nuestros estados, que se podría hacer extensible en este campo.

Con respecto al resto de la región podemos notar el desarrollo en cuanto a materia de Defensa y prevención de ciber ataques a Colombia dado el marco de conflicto que viene sosteniendo desde hace años en su territorio y la colaboración con la que cuenta por parte de Estados Unidos en materia de defensa en general.

Con respecto a la República de Chile, hasta la fecha manifiesta un estado insipiente en cuanto a regulaciones y adquisición de equipos para la realización de operaciones ciber, pero poseen una estructura preestablecida de Inteligencia Nacional que le da un marco acorde para desarrollar capacidades en materia de operaciones en este ámbito en menos de 5 años de manera eficiente y eficaz.

Con respecto a los ejemplos de hechos acontecidos en materia de ciber ataques, las fechas de principio de siglo, fueron colocadas adrede para demostrar que desde hace más de veinte años este espacio transversal es utilizado por los estados y organismos para o supraestatales para lograr sus metas de maneras subrepticias y con la cierta facilidad que este nuevo espacio les brinda para deslindarse de las responsabilidades.

CAPÍTULO 2

Posible determinación de la organización de un elemento de ciberinteligencia a nivel TO.

El objeto de este capítulo es determinar la posibilidad de contar con una organización de ciberinteligencia para el TO, para lo cual se tendrá en cuenta las necesidades y los alcances de esta, la determinación de la misión general, su concepto de empleo y su diseño definitivo.

Se estructura en tres secciones, siendo en la primera de ellas donde se abordan los conceptos generales; mientras que en una segunda sección se determinará el objetivo, misión, organización, funciones y actividades. En una tercera sección se desarrollará un concepto de empleo, capacidades y limitaciones. Para cerrar luego con las conclusiones parciales del capítulo.

SECCIÓN I

Conceptos Generales

La ciberinteligencia apoyará a la ciberdefensa contrarrestando los esfuerzos de inteligencia de los ciberactores que busquen afectar negativamente la infraestructura, reputación y personal de las Fuerzas Armadas. En la actualidad, la capacidad de desarrollar un esfuerzo de ciberinteligencia, no se encuentra limitada a los Estados, existiendo actores no estatales que constituyen amenazas o riesgos y que cuentan con capacidades de consideración.

El área de la ciberinteligencia es aquella donde se desarrollan actividades que son totalmente concurrentes y perfectamente coordinadas con la ciberdefensa, con el objetivo de identificar, definir, clasificar y cuantificar ciberamenazas, reales o potenciales. Se nutre de la información obtenida por los sistemas de ciberdefensa, del análisis de fuentes abiertas, nuevas ciberamenazas y nuevas tendencias de ciberataques para la obtención de inteligencia que será fundamental en el éxito de las operaciones de ciberdefensa permitiendo complementariamente la readecuación de las políticas de seguridad y la determinación de estándares de comportamiento seguro en la generación de nuevas reglas y métricas de los sistemas de monitoreo y alarma, en la prevención ante ciberataques.

Su ejecución es de carácter permanente, manifestándose principalmente en la obtención de información, pero no necesariamente se limitará a ella. Esta información estará orientada a la producción de inteligencia para servir a los máximos niveles de decisión y a brindarle ventajas durante el desarrollo de actividades de ciberdefensa.

La ciberinteligencia es un procedimiento de inteligencia realizado en o desde el ciberespacio que, mediante la adquisición y el análisis de información para identificar, rastrear y predecir las capacidades, intenciones y actividades de Estados o ciberactores, con la finalidad de apoyar la toma de decisiones del Comandante Operacional.

Desde el punto de vista de las operaciones militares, el ciberespacio es una de las cinco dimensiones de operaciones que es transversal a todas las demás a saber: tierra, mar, aire y el espacio (espectro electromagnético), y que son interdependientes. El objetivo central de la integración de estas dimensiones es aprovechar sus capacidades para crear efectos únicos y, posiblemente, decisivos.

En consecuencia, las principales amenazas pueden tener las siguientes características: a) El atacante puede estar en cualquier parte del mundo; b) La confrontación en el ciberespacio presenta características similares de un conflicto asimétrico; c) Permite obtener información de forma anónima; d) Evoluciona rápidamente siguiendo el avance tecnológico de las TICs; e) La ciberguerra obtiene resultados importantes a bajo costo.

Para lograr una ciberdefensa efectiva que prevenga, anticipe, identifique y localice ataques y amenazas, es necesario ejecutar actividades de inteligencia en el espacio cibernético con el fin de obtener y analizar la información sobre los componentes antes nombrados.

De esta manera, la ciberinteligencia se plasma en el conjunto de operaciones complementarias a las operaciones ofensivas y defensivas, llevadas a cabo en el ciberespacio, en el contexto de la planificación de la Estrategia Nacional, coordinada e integrada por el Ministerio de Defensa, con el propósito de proteger los sistemas de información de interés, obtener información de interés para la producción de Inteligencia y comprometer la eficacia de los sistemas de información del oponente/adversario.

La ciberinteligencia contribuye a la prevención de los ataques cibernéticos determinando presentes y futuras amenazas minimizando así la posibilidad de incidencias contra los activos establecidos por el escalón superior y contribuyendo a las actividades de ciberdefensa.

SECCIÓN II

Objetivo, Misión, Organización, Funciones y Actividades

En cuanto a los objetivos de un elemento de Ciberinteligencia dependiente del Comando Conjunto de Ciberdefensa fijaremos los siguientes: a) Disponer de alertas tempranas relativas a ciberamenazas a través del análisis de los datos e información obtenidos previamente; b) Conocer las características de las ciberamenazas para monitorizar y neutralizar su impacto, así como reducir las debilidades y reforzar las fortalezas; c) Contribuir con los procesos de decisión en materia de seguridad y ciberseguridad mediante la reducción de la incertidumbre; d) Determinar el Orden de Batalla (OB) cibernético de los diferentes actores.

Como Misión del elemento de ciberinteligencia será obtener información y producir inteligencia operacional al ciberespacio, en todo tiempo, para conocer las capacidades, debilidades e intenciones de un actor de interés a fin de contribuir con la planificación y ejecución de las operaciones de Nivel Operacional y eventualmente Estratégico para evitar la sorpresa. Para lograr esta misión deberán contar con enlaces permanentes con los elementos de Ciberinteligencia de cada fuerza, que en la actualidad tal como en este nivel operacional aun no existe ni una organización de este tipo, a pesar de contarse con varios trabajos similares a este y diversos proyectos presentados por cada una de las Fuerzas.

En lo referido a la organización y el personal requerido para cubrir esos puestos podemos expresar que la jefatura tendrá la misión de dirigir sus operaciones de acuerdo con las órdenes y directivas del Comando Conjunto de Ciberdefensa, será conveniente que el puesto sea ocupado eventualmente por un oficial Superior, o idealmente por un Oficial Jefe con la aptitud especial de Inteligencia de cualquiera de las tres Fuerzas, con respecto a las necesidades de este nivel es conveniente que dicho elemento sea de nivel Unidad, o sea un Batallón de Ciberinteligencia Conjunto.

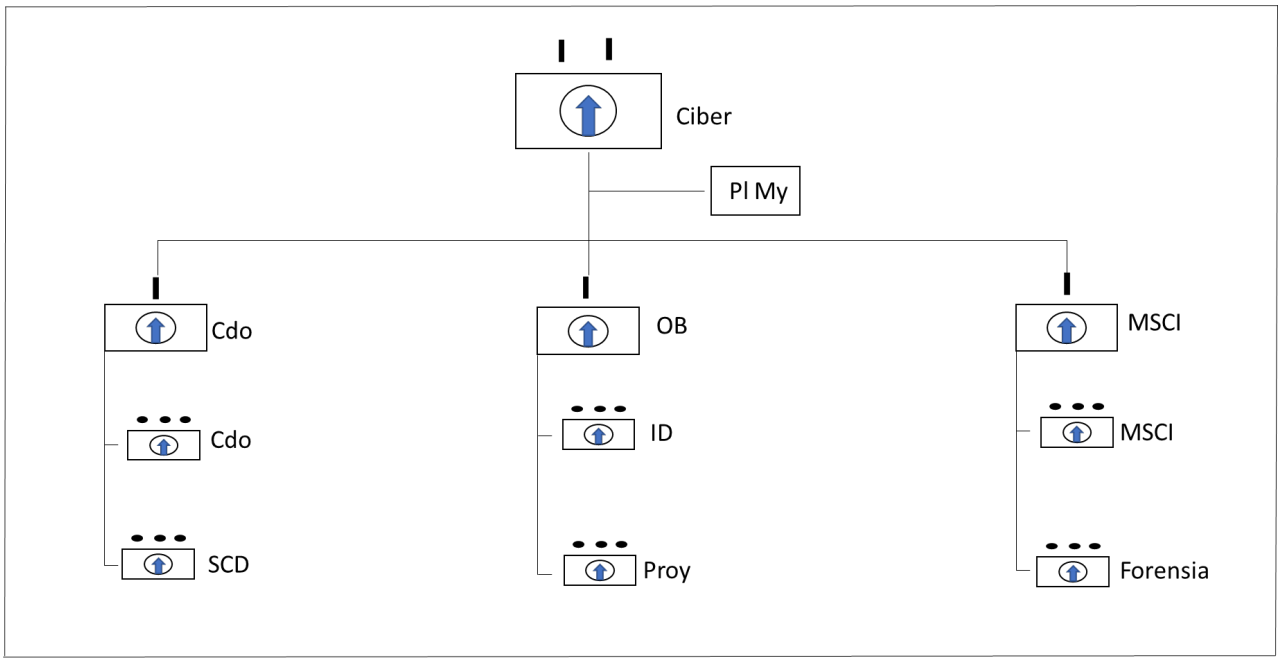


Gráfico N°3 (Organización propuesta de B Ciber Icia Conjunto)

El cuanto al segundo Jefe de Elemento es menester que sea un Oficial Jefe de cualquiera de las FFAA con la capacitación de Ingeniero Militar especialista en Informática o en su defecto formado por el Instituto de Ciberdefensa de las FFAA (ICFFAA), se desempeñará como Jefe de plana mayor de la Unidad, que será a semejanza de cualquier Unidad Conjunta siendo sus puestos ocupados por personal especialista de la diferentes áreas de la conducción.

Dicho elemento contará con tres subunidades a saber: Compañía Comando, Compañía Orden de Batalla y Compañía Medidas de Seguridad y Contra Inteligencia.

La Compañía Comando podrá ser conducida por un Oficial subalterno especialista en Sistema de Cómputos de Datos (SCD) o sus equivalentes de acuerdo a la Fuerza de la que se trate. Esta subunidad se encargará de las tareas y funciones de mantenimiento en general, asistiendo a la Plana Mayor en el desarrollo de sus funciones, en cuanto a la Sección SCD será la encargada del mantenimiento y funcionamiento de los equipos específicos, almacenamiento de datos y mantenimiento del Server de la Unidad, debiéndose contar con un Oficial SCD y cuatro Suboficiales auxiliares especialistas en SCD.

La Subunidad Orden de Batalla deberá ser conducida por un Oficial subalterno con la Aptitud especial de Inteligencia, contará con dos Secciones a Saber:

La sección Identificación (ID) llevará acabo las tareas de determinación de los incidentes producidos en todas las redes de las fuerzas, de manera de intentar identificar a los agresores de acuerdo a sus tácticas y procedimientos de empleo y los demás factores del Orden de Batalla, de esta forma proporcionar información a los canales técnicos de estas amenazas reales y potenciales. En cuanto al personal, los puestos de analistas pueden ser cubiertos por Personal Civil de Inteligencia (PCI) especialistas en ciber o en seguridad informática, siendo sus Jefes de Grupo y coordinadores de sus tareas Suboficiales especialistas en Inteligencia o en Ciberdefensa indistintamente.

La sección Proyección (Proy) contribuirá con los Comandos de Ciberdefensa con el ciber patrullaje defensivo y de proyección para lo cual serán grupos dentro de la sección con equipos de analistas especialistas en la operación y nociones de desarrollo de software, con este accionar permitirá a la Subunidad en su conjunto proporcionar a las Fuerzas el OB cibernético. Con respecto al personal para cubrir los puestos internos, es similar a lo antes expresado también pudiendo contar con Soldados Voluntarios que sus conocimientos le permitan cumplir con los roles requeridos.

En Cuanto a la Compañía MSCI, además de trabajar en forma conjunta y coordinada con la subunidad arriba nombrada debe ir actualizando las pautas a medida que se vayan subsanando y detectando diferentes vulnerabilidades de las redes inherentes a las FFAA y estructuras criticas estratégicas, para ello contará además de la sección específicamente dedicada a velar por las medidas de seguridad con otra que se encargue de la forensia de los equipos y redes involucrados en diferentes incidentes. El después, o las acciones que se toman una vez ocurrido el incidente informático, algunas tareas relacionadas con este ámbito incluyen la recuperación de datos borrados, el análisis de ingeniería inversa,

la identificación de metodologías utilizadas para explotar el sistema, en está etapa cuenta con la participación activa de la Sección OB, que es posible que confirme o identifique un nuevo agresor o sus procedimientos, el jefe de Sección deberá ser un Oficial Ingeniero Informático y los jefes de grupo suboficiales auxiliares de inteligencia o auxiliares en ciberdefensa.

Este Batallón deberá estar en capacidad de cumplir con las distintas Funciones como ser: a) Identificar vulnerabilidades potenciales y reales de los propios sistemas y/o activos críticos de información nacional que sean asignados para su protección por parte del CCCD; b) Detectar filtraciones de información; c) Identificar y mitigar ciberamenazas potenciales y reales en canales de comunicación y cualquier otro medio que curse información; d) Identificar actores y ciberactores potenciales y reales de interés para la protección de los propios sistemas y/o activos críticos de información nacional que sean asignados para su protección por parte del CCCD; e) Identificar posibles aliados y compartir datos para crear una comunidad de ciberinteligencia.

Las actividades de ciberinteligencia constituirán una herramienta fundamental en la configuración y determinación de probables amenazas, definiendo este dominio como una evolución exponencial que busca anticiparse a las recientes tecnologías empleadas como amenazas, que son elaboradas con herramientas que buscan ocultarse permanentemente a los sistemas de monitoreo.

Se destacan las siguientes actividades: a)Patrullaje cibernético consiste búsqueda de información en fuentes abiertas en el ciberespacio; b) Identificación de ciberamenazas; c)La determinación de posibles tácticas, procedimientos y técnicas de empleo y comprende los aspectos que resumirán la metodología del accionar de los ciberactores, sintetizando el "cómo" se prevé que estos lleven adelante las ciberamenazas; d) Proyección de ciberataques consiste en determinar potenciales ataques y los efectos que de ellos se pudieren derivar en un corto-mediano plazo; e) Simulación de ciberataques para contribuir a la seguridad de la fuerza mediante simulacros de ciberataques de manera similar a los empleados por ciberactores de interés con la finalidad de determinar fortalezas y debilidades; f) Forensia informática que tiene por finalidad adquirir, preservar, obtener y presentar datos que han sido procesados electrónicamente y/o soportes informáticos.

Gráfico N°4 (Actividades de Ciberinteligencia, CT GARRUBA J,M - CIM)

SECCIÓN III

Concepto de empleo, capacidades y limitaciones

Es inexorable recurrir nuevamente a la relación con la ciberdefensa, que tiene como objetivo neutralizar todas aquellas amenazas que pudieran afectar la integridad, disponibilidad y confidencialidad de la información a través del ciberespacio. Debe ser capaz poder potenciar las capacidades militares para ejercer la respuesta oportuna, legítima y proporcionada en el ciberespacio ante amenazas o agresiones que puedan afectar a la Defensa Nacional.

Las actividades relacionadas a la ciberdefensa deben ser desarrolladas de forma sistemática por personal especializado que domine los métodos, procedimientos y vocabularios inherentes. Desde el punto de vista de las operaciones militares, el ciberespacio es una de las cinco áreas o dimensiones de operaciones que penetra todas las demás ya mencionadas (tierra, el mar, el aire y el espacio); y que son interdependientes.

Existe una estrecha relación entre la ciberdefensa, la ciberinteligencia, la ciberseguridad y la Seguridad Informática, que se basa en la necesidad de interactuar mediante un cuerpo normativo, procedimientos e intercambio de información que sirve a todos las áreas que cumplen sus funciones y desarrollan sus operaciones en el ciberespacio.

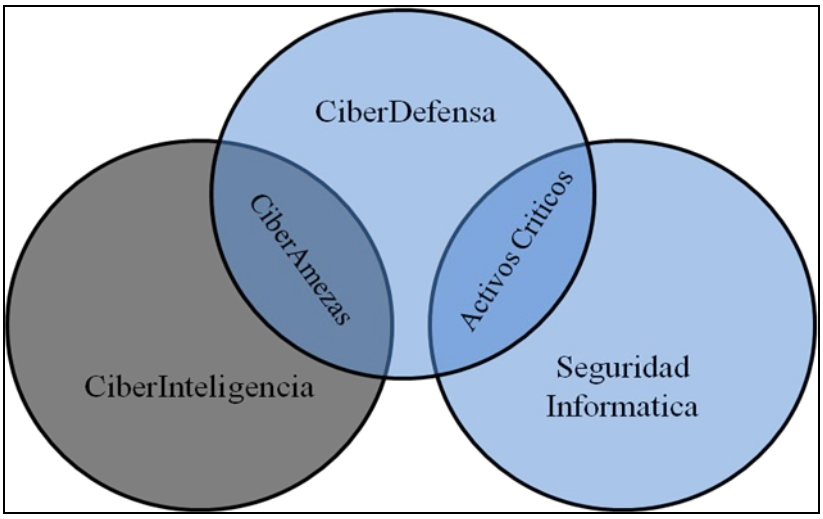


Gráfico N° 5 (Relación con la Cibdef y Seg Info)

La seguridad informática es el conjunto de técnicas y herramientas que se utilizan para proteger la información procesada, enviada, transportada y almacenada en cualquier dispositivo informático. La misma, posee un alcance mayor que la ciberseguridad, puesto que la primera busca proteger la información de riesgos que puedan afectarla, en sus diferentes formas y estados y se sustenta de metodologías, normas, técnicas, herramientas, estructuras organizacionales, tecnología y otros elementos, que soportan la idea de protección en las distintas facetas de la información; también involucra la aplicación y gestión de medidas de seguridad apropiadas, a través de un enfoque general.

Por consiguiente, se puede determinar que resulta necesario contar con un alto grado de integración de la información entre las dos disciplinas. La finalidad de dicha integración será lograr la eficiencia en el producto final y utilidad que éste tendrá para responder los vacíos de información con la mejor capacidad disponible y la comprensión de los resultados esperados.

Para una defensa eficiente frente a un ciberataque, la responsabilidad de analizar y obtener información relevante para la toma de decisiones resulta fundamental, siendo ésta la finalidad de la ciberinteligencia: obtener información para la determinación de amenazas para proponer una mejor respuesta, utilizando herramientas necesarias y personal idóneo.

La ciberinteligencia es un área concurrente y se nutre de la información obtenida por los sistemas de ciberdefensa, del análisis de fuentes abiertas, nuevas ciberamenazas y tendencias de ciberataques para la producción de inteligencia que será fundamental en el éxito de las operaciones de ciberdefensa permitiendo complementariamente la readecuación de las políticas de seguridad y la determinación de estándares de comportamiento seguro en la

generación de nuevas reglas y métricas de los sistemas de monitoreo y alarma, en la prevención ante ciberataques.

En cuanto a las capacidades que debe desarrollar nuestra organización se pueden enumerar las siguientes: a) Explotar publicaciones especializadas; b) Buscar patrones de ataque en pizarras, foros y sitios especializados; c) Detectar e identificar actores y ciber-actores de interés; d) Monitorear información de interés en mercados y foros de interés; e) Detectar nuevas tendencias en ataques informáticos; f) Analizar incidentes origen internos o externos que afecten a las Fuerzas; además se pueden destacar la realización de otro tipo de actividades a saber: a) Detectar la difusión de publicaciones y documentos que afecten la seguridad de las Fuerzas; b) Obtener y explotar fuentes de información abiertas profundas; c) Instrucción a otros Elementos de las Fuerzas; d) Participar en la obtención de información mediante metodologías de Forensia informática.

En cuanto a las limitaciones mencionaremos las siguientes: a) Limitada capacidad en la obtención y procesamiento de la información; b) Escasa capacidad de adaptarse a la constante evolución tecnológica; c) Limitada capacidad de comprensión de la información en distintos idiomas; d) Personal altamente capacitado y difícil reemplazo.

Estas últimas mencionadas se van a ver afectadas en gran medida de acuerdo a los sistemas con los que se cuenten y el equipo de dotación de la Unidad.

Conclusiones Parciales

Así como en todas la operaciones militares intervienen los diferentes campos de la conducción, dentro de las operaciones ciber cobra fundamental importancia el área de inteligencia; por ello se han presentado diferentes proyectos de reglamentos a nivel especifico de cada fuerza y conjunto, donde por añadidura se plantea la necesidad de contar con una organización dentro de cada componente dedicada a las actividades de inteligencia dentro del ciberespacio, coordinado especialmente sus funciones y responsabilidades con el Comando Conjunto de Ciberdefensa y dentro de los componentes con el arma de Comunicaciones o sus equivalentes para de esta forma lograr la eficiencia y eficacia en dichas operaciones.

Queda en claro que el factor crítico de esta nueva organización va a ser el personal de especialistas necesarios para desempeñarse en las diferentes dependencias de la organización. En este apartado cabe mencionar que dentro de los recursos humanos con que cuentan la FFAA se cuentan en esta materia un centro de desarrollo de software, donde cualquier elemento que tenga responsabilidades dentro del ciberespacio, no sólo, debería apoyarse y coordinar; sino que este elemento va a formar parte importante en las constantes actualizaciones necesarias para llevar a cabo las funciones y tareas de ciberinteligencia.

Desde el punto de vista del área de personal en la actualidad el EMCO carece de infraestructura y de las herramientas para el personal que sea destinado en caso de ponerse en funcionamiento una Unidad dependiente.

Será necesario para la organización propuesta contar al menos con un Oficial Ingeniero Militar (OIM) Ingeniero informático en puestos donde se requiera más especialización. Las Fuerzas cuentan dentro de sus recursos humanos especialistas en la materia, incluso contando con instituciones de formación como la Facultad de Ingeniería del Ejercito (FIE) y sus similares en la Armada y en la Fuerza Aérea.

Continuando con la importancia de la capacitación de los analistas que se requieren para formar parte de esta organización propuesta, es relevante el conocimiento en idiomas de los mismos, incluso, idiomas que no son de dominio común en occidente, tales como el chino y el ruso.

Como factor de contingencia a destacar es el entorno, conducción centralizada y la ejecución descentraliza, esto le permitirá no solo al jefe de Unidad, sino que, a los jefes de Compañía, tener la capacidad de conducir a las suyas respectivas en un ambiente operacional complejo tendiendo al caos, donde las amenazas que deberán afrontar aparte de ser hostiles, serán dinámicas y de muy difícil identificación. Esta Unidad deberá estar en capacidad de neutralizar las amenazas e identificar a los ciberactores, dando paso, de esta manera, a

efectuar las denuncias correspondiente y transferencia de información obtenida a la dependencia de ciberinteligencia criminal que corresponda.

Con respecto a los parámetros de diseño será importante destacar la toma de decisiones que se producirá en la Unidad, donde según sea la decisión y la prioridad de la superioridad, podrá diversificarse en las subunidades que la conforman, dándole una mayor complejidad en el ejercicio del comando.

Conclusiones Finales

Durante el desarrollo de la presente investigación, no se ha realizado un análisis del marco legal ya que se desarrolla en múltiples trabajos de la temática y todo lo planteado en el trabajo se ajusta a las leyes y normas vigentes, situación de las organizaciones en otros estados, los medios que emplean y finalmente con estos antecedentes determinar una organización de ciberinteligencia a nivel Teatro de Operaciones. Por esto es importante detallar aspectos que sobresalen del desarrollo.

En primer lugar, se observa desde el punto de vista de la "voluntad política", cierta displicencia en los temas que hacen al área de defensa en general, ya que, desde el dictado de la ley en el año 1988, pasó más de una década hasta la promulgación de la Ley de inteligencia en 2001. Así como las reglamentaciones de las mismas, que, en el mejor de los casos, deja muchos grises y vacíos legales, dejando dudas, sobre todo, del límite claro entre defensa y seguridad.

Específicamente en lo que refiere a la ciberseguridad y ciberdefensa, fue mencionado como primera noción del tema en el Libro Blanco de Defensa del año 1998 y desde ese tiempo hasta el año 2011 no se llevó a cabo ni una acción, recién en ese año se volvió a retomar el tema por parte de las autoridades, donde finalmente en el año 2014 se ordenó la conformación del Comando Conjunto de Ciberdefensa con la misión de ejercer la conducción de las operaciones dentro de este ámbito en forma permanente a los efectos de garantizar las operaciones militares del instrumento militar de la defensa nacional en cumplimiento de su misión principal y de acuerdo a los lineamientos establecidos en el planeamiento estratégico militar.

Desde su conformación hasta nuestros días se han presentado proyectos de reglamentos de ciberinteligencia, que aún no han sido aprobados, tanto a nivel conjunto como específico de las Fuerzas, pero en ninguna instancia se propuso la conformación de una organización para cumplir estas misiones específicas de ciberinteligencia, lo que dio origen al presente trabajo.

Con respecto al tratamiento que recibe el tema en las potencias pioneras en el ciberespacio, cabe destacar que sus desarrollos vienen en marcha desde la primera década del presente siglo; es por esto que se los tomó como casos de estudio por la experiencia y el uso de materiales, que han ido evolucionando tanto o más que los potenciales agresores, ya que en el campo de la inteligencia la anticipación es fundamental.

También consideramos importante destacar ciertos sistemas y sus respectivos softwares para el desarrollo de las actividades específicas de ciberinteligencia, y como estas

nuevas tecnologías no sólo son aplicables en el ámbito de defensa o seguridad, sino que también cada vez más a la vida cotidiana de los ciudadanos, es por ello, que las personas tienen acceso a ella con mínimos implementos se pueden constituir en potenciales ciberactores.

Dentro de los estados actores dentro del marco regional, es menester fomentar la cooperación en materia de ciberdefensa con la República federativa del Brasil, ya que no sólo cuenta con las organizaciones y materiales bien determinados desde comienzos de la segunda década del siglo; sino, que cuenta con varios proyectos y un todavía insipiente desarrollo de tecnología propia, de esta manera pretende no depender de la buena voluntad de un tercero a la hora del desarrollo de un potencial ciberconflicto. También dentro de esta política estatal cuenta con empresas del estado dedicada a la producción de hardware y software para la defensa.

En materia del estudio de casos hemos observado como llevan a cabo su política de ciberinteligencia otros Estados soberanos, destacamos el caso del Reino Unido de Gran Bretaña e Irlanda del Norte, ya que dentro de las organizaciones ciber, cuenta con la 6ta División (Creada a mediados del año 2019), una División de Guerra Cibernética para centrarse en las amenazas digitales en el Marco del Componente Terrestre. Constituye un elemento a ser tomado en cuenta a la hora de articular la ciberinteligencia a nivel Operacional y Táctico.

Una vez estudiado nuestro marco legal el desarrollo de las organizaciones de ciberdefensa de otros estados y el análisis del contexto tanto nacional como internacional, podemos vislumbrar y proponer una organización de ciberinteligencia de nivel Unidad dependiente directamente del Comando Conjunto de Ciberdefensa.

Como ya fue expresado en las conclusiones parciales del capítulo correspondiente es menester analizar los factores inherentes al entorno, el cual, aún no tiene reglas claras o límites tridimensionales, haciéndolo naturalmente caótico. a los efectos de tenerlos especialmente en cuenta a la hora de diseñar un cuadro de organización, así como también para la selección y capacitación del personal con la máxima especialización requerida por este complejo ámbito.

En este ambiente en particular van a primar la conducción centralizada y la ejecución descentralizada, flexible y coordinada, no sólo en el ámbito interno de la organización, sino también, con las Direcciones de Comunicaciones e Informática de las tres FFAA, El Comando Conjunto de Ciberdefensa y estrechos vínculos con los organismos de

ciberinteligencia criminal, para derivar los casos que dependan de este ámbito, sin perjuicio de efectuar las denuncias correspondientes.

Por lo expresado en el párrafo anterior es de vital importancia que el personal a ser designado, desde el Jefe del elemento hasta el último analista, cuenten con un perfil personal y profesional acorde a la importancia de la misión de la Unidad propuesta por este trabajo.

Un párrafo aparte y que es una situación a considerar para futuros estudios es el de la adquisición de material para la organización presentada; ya que dentro de la triada doctrina, organización y equipo; este trabajo guardó como finalidad ulterior presentar una Unidad de ciberinteligencia, para lo cual indefectiblemente se vieron los aspectos referidos a la doctrina anteriormente mencionada y someramente materiales y equipos utilizados por otros actores a nivel Táctico, Operacional y Estratégico.

Se pretende dejar precedente para la creación del citado elemento, modificación y futura aprobación de diferentes proyectos de reglamento de Ciberinteligencia presentados a los diferentes Estados Mayores y en el EMCO, y como corolario final del proyecto; una vez analizada la doctrina y determinación final de la organización; proceder a un estudio específico y exhaustivo del material o materiales adquirir.

Por último, destacar la capacidad, no sólo, a nivel Estado, sino, a nivel Fuerzas Armadas del desarrollo de software. Este aspecto, no sólo permite bajar los costos de los futuros desarrollos, sino que, también contribuye a un mejor asesoramiento profesional a la hora de adquirir los materiales necesarios en materia de hardware y lograr independencia y una mayor seguridad informática.

Referencias

Doldán Estrada, F. J. (2014) Diseño de un subsistema de inteligencia conjunto para el apoyo meteorológico en el nivel operacional.

De VERGARA, E y TRAMA, G (2017). Operaciones Militares Cibernéticas: Planeamiento y Ejecución en el nivel Operacional.

INSA (2011). Cyber Intelligence: Setting the Landscape for an Emerging Discipline. The Intelligence and National Security Alliance. Cyber Intelligence White Paper.

Estado Mayor Conjunto. (2005) Reglamento de Doctrina Básica para la Acción Militar Conjunta del EMCO (RC 00-01).

Estado Mayor Conjunto. (2012) Reglamento de Informática para la Acción Militar Conjunta del EMCO (RC 21 -01).

Ejército Argentino. (2007) Destacamento de Inteligencia de Combate (ROP 11 – 04).

ARQUILA, J., y RONDFELD, D. (2003). Redes y guerras en red. El futuro del terrorismo, el crimen.

TOFFLER, A. y H. (1994). Las Guerras del Futuro, la supervivencia en el alba del siglo XXI.

CUBEIRO, E (2016). Ciberinteligencia. DIAZ, Antonio (Ed). Conceptos Fundamentales de Inteligencia.

SANCHEZ HERRAEZ, P. (2014). La Nueva guerra Híbrida: un somero análisis estratégico.

CASARINO, P. (2018). Ciberdefensa una opinión personal, Manual de Informaciones.

CASARINO, P.G y ORTIZ, J.U (2019). La Ciberdefensa y la Ciberinteligencia Militar.

Ley 23.544/88 de Defensa Nacional

DAPENA, Nicolás (2007) “La diferencia entre seguridad interior y defensa nacional. Conceptos, competencias, y una propuesta facultades, límites, prohibiciones e interacciones.

http://servicios.infoleg.gob.ar/infolegInternet/anexos/20000-24999/20988/texact.htm

Ley 23.544/88 de Defensa Nacional
http://servicios.infoleg.gob.ar/infolegInternet/anexos/20000-24999/20988/texact.htm

Ley 25520/01 Ley de Inteligencia Nacional
http://servicios.infoleg.gob.ar/infolegInternet/anexos/70000-74999/70496/texact.htm

Resolución 385/13 Jefatura de Gabinete de Ministros
https://www.argentina.gob.ar/jefatura

El Ministerio de Defensa de la República Argentina, Resolución Ministerial Nro. 343 del 14 de mayo de 2014

https://www.fuerzas-armadas.mil.ar

Decreto 571/2020 Defensa Nacional

https://www.boletinoficial.gob.ar/detalleAviso/primera/231293/20200629

DIRECTIVA DE POLÍTICA DE DEFENSA NACIONAL (DPDN) Decreto 457/2021

https://www.boletinoficial.gob.ar/detalleAviso/primera/246990/20210719

ARPAGIAN, N. (2009). La Cyberguerre, la guerre numérique a comencé. Ed Magnard-Vouibert. París y reportaje (2010)

http://www.pagina12.com.ar/diario/ elmundo/4-145379-2010-05-09.html

Página Oficial del Gobierno del Reino Unido de Gran Bretaña e Irlanda del Norte

https://www.gov.uk

Política de Ciberdefensa de la República de Chile

https://obtienearchivo.bcn.cl/obtienearchivo?id=repositorio/10221/26760/1/POLITICA_NACIONAL_DE_CIBER.pdf

Anexos

Anexo 1: Glosario de términos.

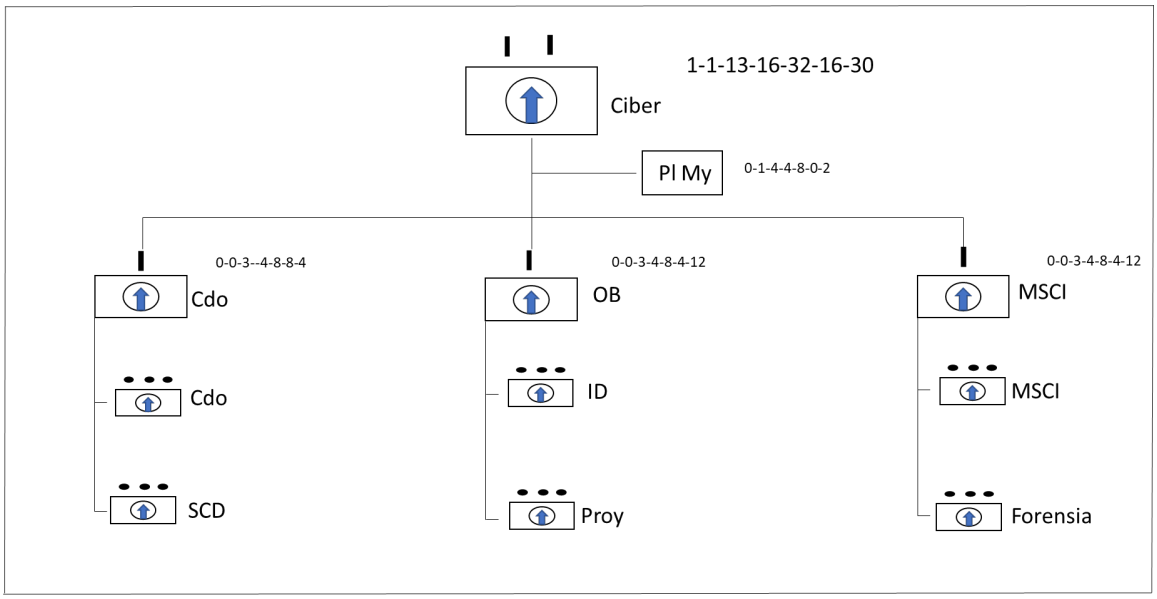
1. Ciberespacio: Es el conjunto de medios y procedimientos basados en las Tecnologías de la Información y la Comunicación (TICs) configurados para la prestación de servicios. Está constituido por hardware, software, Internet, servicios de información y sistemas de control que garantizan la provisión de aquellos servicios esenciales para la actividad de cualquier Estado, en especial aquellos ligados a sus infraestructuras críticas.
2. Ciberactores: persona, organización o Estado que posee un objetivo, motivación y recursos para hacer daño buscando una oportunidad para explotar una vulnerabilidad. Se identifican los siguientes tipos:
    a. Grupos delictivos.
    b. Grupos terroristas.
    c. Grupos subversivos.
    d. Estados hostiles.
    e. Hackers aislados.
    f. Competencia (ciber-espionaje).
3. Ciberamenazas: Circunstancia desfavorable que puede ocurrir a los sistemas y servicios presentes en el ciberespacio o alcanzables a través de éste y que cuando sucede tiene consecuencias negativas sobre los activos provocando su indisponibilidad, funcionamiento incorrecto o pérdida de valor. Una ciberamenaza puede tener causas naturales, ser accidental o intencionada.
4. Ciberataque: actividad maliciosa realizada a través del ciber-espacio con la finalidad de destruir la integridad, confidencialidad y disponibilidad de datos, robar información clasificada o perturbar, desactivar, destruir o controlar un entorno o infraestructura de cibernética.
5. Ciberinteligencia: procedimiento de inteligencia realizado en o desde el ciberespacio, desarrollando actividades que son totalmente concurrentes y perfectamente coordinadas con la ciberdefensa, buscando identificar, definir, clasificar y cuantificar ciberamenazas, reales o potenciales para su identificación, rastreo y determinación de capacidades, intenciones y actividades de Estados o ciberactores en el ciberespacio de interés, y que de manera complementaria, permita obtener información que contribuya

al planeamiento de operaciones convencionales, aunque no esté necesariamente relacionada a capacidades cibernéticas.

6. Ciberseguridad: En el concepto más básico es la preservación de la confidencialidad, integridad y disponibilidad de la información en el ciberespacio. Es la actividad, proceso, capacidad, o estado deseado en el que los sistemas de información, redes de transmisión de datos, medios de comunicaciones e informática y los activos de información, están protegidos o pueden defenderse contra daños, usos o modificaciones no autorizadas.
7. Patrullaje cibernético: búsqueda de toda información pública que se encuentre alojada en la web relacionada o sobre una temática determinada previamente preestablecida.
8. Infraestructuras críticas: Son aquellas que resultan indispensables para el adecuado funcionamiento de los servicios esenciales de la sociedad, la salud, la seguridad, la defensa, el bienestar social, la economía y el funcionamiento efectivo del Estado, cuya destrucción o perturbación, total o parcial, los afecte y/o impacte significativamente, pero que no necesariamente están relacionadas con las Tecnologías de Información (IT) o Tecnologías de Operaciones (OT).
9. Activos Críticos de Información: Es aquel activo de información que proporciona un servicio esencial, cuyo funcionamiento resulte indispensable para el cumplimiento de las funciones de la organización. Aquel activo que es soporte necesario para el cumplimento de una función o procesos, hereda la criticidad del Activo Crítico de Información, como por ejemplo instalaciones edilicias y equipamiento auxiliar (grupos electrógenos, aires acondicionados, etc.).

Fuentes: Convenciones internacionales sobre las definiciones y documento expedido por la OTAN sobre el dominio del ciberespacio (NATO Bi-SC Initial Assessment of Recognising Cyberspace as a Domain).

Anexo 2: Cuadro de organización del Batallón de Ciberinteligencia Conjunto.



Fuente: Elaboración Propia.