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

UNDEF
Universidad de la Defensa Nacional

TRABAJO FINAL INTEGRADOR

Título: "La Ciberdefensa como factor crítico en el desarrollo de Operaciones Militares en el Nivel Operacional".

Que para acceder al título de Especialista en Conducción Superior de OOMMTT presenta el Mayor CARLOS GERARDO CASALE

Director de TFI: LICENCIADA MAGISTER PATRICIA LUSSIANO

Ciudad Autónoma de Buenos Aires, de noviembre de 2022.

Resumen

Los adelantos tecnológicos surgidos de la revolución tecnológica, producto de la revolución industrial, dieron nacimiento a las Nuevas Tecnologías de la Información y la Comunicación y su influencia creciente en el campo de combate moderno. Estas permiten transmitir y recibir un gran volumen de información a través del ciberespacio, nuevo dominio de la guerra que cruza en forma transversal a los ya conocidos (terrestre, marítimo, aéreo y aeroespacial), el cual mediante su afección puede generar un cambio en la dirección de las operaciones y en la toma de decisiones. Es por esto que el Ciberespacio ha pasado a conformarse como un nuevo escenario.

El presente trabajo de Investigación, tiene el propósito de determinar cuál podría ser el proceso de trabajo y que organización podría concretarlo, en el nivel táctico, permitiendo el desarrollo de Operaciones de Ciberdefensa dentro del Componente Terrestre del Teatro de Operaciones. Se comenzó con el planteo de un problema y a continuación se estableció los objetivos que dan respuesta a él. Inicialmente se efectuó un análisis del plexo normativo nacional vigente, que regula el empleo del Ciberespacio y las operaciones que se ejecutan en él, para definir las limitaciones y responsabilidades; basado en el análisis de la Ley de Defensa Nacional, Ley de Seguridad Interior y la Directiva de Política de Defensa Nacional. Posteriormente se determinaron las amenazas y/o riesgos a enfrentar en el nivel de la táctica superior a fin de determinar cuales podrán ser las infraestructuras críticas u objetivos, a afectar por parte del enemigo mediante las Operaciones de Ciberdefensa. Por último se determinó, en base al marco legal, las amenazas establecidas y el análisis de diferentes hechos históricos, el propósito del presente trabajo.

Palabras claves Ciberdefensa, Ciberespacio, Operaciones, Normas, Proceso, Organización.

Índice de contenidos

Índice de Figuras

Introducción

Presentación del Problema

El tema desarrollado en el presente trabajo de investigación aborda la temática para determinar, en base a doctrina nacional y extranjera de carácter público, cual y cómo podría ser el proceso de trabajo que permita llevar a cabo las operaciones de Ciberdefensa dentro del Componente Terrestre y que elemento lo concretaría. Esto se debe a que en el ámbito específico como el conjunto no se cuenta con doctrina rectora sobre este tema de relevancia actual y real dentro del ambiente táctico. Por lo que se considera importante indagar y analizar el marco legal vigente relacionado a este nuevo ambiente de operaciones y su regulación, para poder observar las limitaciones y responsabilidades que se le impone al Instrumento Militar. Se desarrollarán conceptos sobre las operaciones de Ciberdefensa, su ámbito de empleo, los posibles objetivos que buscará afectar el enemigo, lo que nos permitirá determinar las posibles amenazas y cómo influirán en el desarrollo de las operaciones y en el proceso de toma de decisiones a través de un método de análisis particular referido a las ciberoperaciones.

Antecedentes y Justificación del Problema

En las últimas décadas del siglo XX comenzó, de manera constante y rápida, una evolución tecnológica que dio inicio a la Era de la información y las comunicaciones; esto facilitó la aparición de las redes digitales mundiales producto de la conectividad. A partir de esta característica se crea, dentro del Ambiente Operacional, un nuevo dominio transversal a los ya conocidos y con gran influencia sobre ellos. Este nuevo ámbito, denominado Ciberespacio, descripto como:

> "un ambiente complejo que resulta de la interacción de personas, software y servicios en internet por medio de dispositivos y redes conectadas. No posee existencia física sino que es un dominio virtual que engloba todos los sistemas de Tecnologías de la Información y Comunicación" (Secretaría de Modernización, 2019).

Lo expuesto exige integrar nuevos conocimientos en la capacitación del personal y la realización de procedimientos particulares que permitan neutralizar o disminuir las amenazas cibernéticas producidas por actores que controlen este dominio, particularmente del personal de Oficiales y Suboficiales subalternos, que tienen la ventaja de haber nacido en la era de la digitalización, por lo que tienen una afinidad natural hacia lo digital.

Como producto de este nuevo dominio aparecen nuevos conceptos en el ámbito de la política de Defensa Nacional, definidos en el anexo II de la Directiva de Política de Defensa Nacional (Ministerio de Defensa, 2018) como Ciberseguridad, Ciberdefensa, Ciberguerra o Ciberoperaciones. La inclusión de estos nuevos términos, como ejemplificaremos más adelante, muestran su importancia y/o relevancia en diferentes oportunidades; en las cuales se llevaron a cabo ciberataques sobre infraestructuras críticas (IICC) que pusieron en riesgo la Seguridad Nacional de los Estados.

A modo de ejemplo podemos citar diferentes casos, el más conocido y uno de los primeros es el del año 2007 en Estonia, uno de los países europeos más informatizados y digitalizados, el cual sufrió ciberataques cuyos objetivos fueron los medios de comunicación, bancos y diversas entidades e instituciones gubernamentales que colapsaron produciendo disturbios e inestabilidad política. Un año más tarde, en el mes de octubre de 2008, Georgia fue atacada en forma masiva mediante la denegación de servicios consiguiendo desconectar numerosas redes y sitios web. También podemos citar otro ciberataque mundialmente conocido fue el que sufrió Irán, en el año 2010, en sus sistemas de control de la central nuclear de Bushehr y del complejo nuclear de Natanz, fueron afectadas en particular las máquinas centrifugadoras para enriquecer uranio, alterando el proceso de centrifugado lo que provoco que giren a una mayor velocidad sin que el operador lo notara en su pantalla de control, y también afecto a otras industrias, mediante la implantación del virus Stuxnet, principalmente al programa atómico del país, retrasándolo en varios años.

Continuando con la búsqueda y justificación de aspectos relevantes relacionados con la investigación, se considera pertinente remitirse a las bases legales a nivel Nacional en materia de Ciberseguridad y Ciberdefensa. El Ministerio de Defensa expresa en el Libro Blanco de la Defensa, año 2015, "la ciberdefensa adquiere relevancia en tanto capacidad estatal de protección y utilización soberana del ciberespacio esencial, vital o necesario para el funcionamiento del instrumento militar, componentes del Sistema de Defensa y las infraestructuras críticas nacionales" (Ministerio de Defensa, 2015). Resalta como ha ido evolucionando y tomando mayor importancia para la Defensa Nacional las actividades en el Ciberespacio en el cual las tecnologías de la información adquieren una importancia relevante para el desarrollo de las operaciones militares.

El marco legal vigente en el que se encuentra comprendido el tema de investigación lo componen los siguientes documentos: Ley de Defensa Nacional, Directiva de Política de Defensa Nacional, Estrategia Nacional de Ciberseguridad Resolución Nro 829/2019, Glosario de términos sobre Ciberseguridad, Resolución 1523/2019, Política de Ciberdefensa Resolución 1380/2019. La evolución rápida y constante de los métodos empleados para realizar operaciones de Ciberdefensa genera amenazas que requieren una actualización constante de las normativas legales para evitar sobrepasar sus límites.

La Directiva de Política de Defensa Nacional sancionada en el 2018 (Decreto Nro 703/2018) establece los lineamientos en materia de política de defensa nacional; determinando, entre sus temas, el desarrollo de capacidades operacionales para afrontar las amenazas y riesgos que de concretarse afectarán los intereses de la nación. Esta directiva contempla al Ciberespacio como un ambiente operacional militar en donde se pueden configurar amenazas. En su Anexo 1 resalta que deben adecuarse sus organizaciones militares al impacto que surge de los nuevos riesgos.

> ” La política de Ciberdefensa debe orientarse a la reducción gradual de las vulnerabili dades que emergen de la informatización de los activos estratégicos de interés para la Defensa Nacional. Contempla la cooperación con otras áreas del Estado que tengan responsabilidad en la política de Ciberseguridad Nacional” (Ministerio de defensa, 2018, p. 18).

Actualmente se encuentra derogada y reemplazada por el decreto Nro 2645/2014 (DPN 2014) que destaca las dificultades para determinar si la afectación de las acciones cibernéticas es una agresión militar externa o no, por lo tanto limita el accionar del instrumento militar en la ejecución de operaciones de Ciberdefensa.

Como contrapartida al párrafo anterior, no ha sido derogada la resolución 1523/2019 con su anexo glosario de términos sobre Ciberseguridad, en donde contempla como ambiente operacional al ciberespacio; al igual que el Comité de Ciberdefensa creado en 2019. Por lo expuesto anteriormente es necesario aunar conceptos en el marco legal y definir si se contempla el empleo del Ciberespacio para fines militares.

En relación con el tema propuesto para la investigación, a partir del establecimiento del marco legal en cuanto al Ciberespacio y su relevancia para la Política Nacional se establece la organización de la Ciberdefensa en las Fuerzas Armadas. Esta se encuentra conformada por el Comando Conjunto de Ciberdefensa (CCCD) dependiente del Estado Mayor Conjunto (EMCO), del cual a su vez dependen cada una de las Direcciones de Ciberdefensa de las FFAA. En lo específico la Dirección de Ciberdefensa del Ejército Argentino es la encargada de conducir las operaciones de esta naturaleza en nuestro ámbito terrestre.

En lo que respecta a la doctrina en el ámbito conjunto se encuentra en revisión el proyecto de Reglamento de Ciberdefensa para la Acción Militar Conjunta (EMCO, 2018). En él se fijan las bases doctrinarias y los criterios-reglas generales y particulares que sirvan de guía

para la solución de problemas militares que involucren la ejecución de operaciones de Ciberdefensa. También determina el sistema jerárquico dentro del ámbito de la Ciberdefensa, y establece solo un control funcional sobre las Direcciones de Ciberdefensa de cada fuerza.

En cuanto a la doctrina específica no posee, hasta el momento, un reglamento particular referido a Ciberdefensa. Este tema es abordado en el reglamento Conducción de las Fuerzas Terrestres en su capítulo VII, Sección XV, el cual la contempla como una operación complementaria, estableciendo su definición, finalidad, planeamiento y ejecución (Ejército Argentino, 2015). Igualmente, el reglamento de Conceptos Básicos sobre Sistemas de Comunicaciones, Informática y Guerra Electrónica de la Fuerza en el capítulo VIII, Sección IX, solo realiza una breve mención en pocas líneas, definiendo "cómo el apoyo de comunicaciones e informática es responsable de instalar y operar los medios que ejecutan las operaciones de Ciberdefensa y la Seguridad Informática con la que se encuentran estrechamente relacionadas". En lo referente a la responsabilidad de las actividades, planeamiento y ejecución, que tengan relación estrecha con las operaciones de Ciberdefensa, le son asignadas al Oficial de Comunicaciones - Informática y Guerra Electrónica (OCIGE) por encontrarse, doctrinariamente, en relación con la seguridad informática (Ejército Argentino, 2016. p. 19).

La Dirección de Ciberdefensa del Ejército Argentino, actualmente, se encuentra en la etapa inicial del desarrollo de un reglamento sobre Ciberdefensa, pero previo a esto ha redactado y se encuentran en vigencia Directivas internas de la fuerza que proveen de lineamientos generales sobre el tema. Podemos nombrar la Directiva Anual de Ciberdefensa Nro 001/21 de la Dir Grl Com Info en la que establece y reúne todas las recomendaciones, estándares y procedimientos generales y particulares, complementarios que norman los aspectos de Ciberdefensa en el ámbito de la Fuerza (Ejército Argentino, 2021) o la Directiva Nro 918/18 Régimen de funcionamiento del Subsistema Informático del Ejercito (SUIE) que tiene la finalidad de

establecer los conceptos rectores que norman el funcionamiento del SUIE, determinando normas de procedimientos, instrucciones, funciones y política de seguridad que rigen el empleo del Subsistema Informático para su cumplimiento; también establece las relaciones de comando, responsabilidades, funciones, actividades y tareas del personal competente en esta área (Ejército Argentino, 2018).

Se observa, tanto en materia conjunta como específica, que se encuentran principalmente en desarrollo y/o revisión proyectos de reglamentos; pero solo se están en vigencias pocas bases doctrinarias. Es por esto, que no se encuentran especificados los procesos de trabajo que permitan llevar a cabo este tipo de operaciones en el Ciberespacio, entendiendo por estos como aquellas actividades de planeamiento y ejecución.

Para el desarrollo de la investigación, se tendrá en cuenta el trabajo "Operaciones Militares Cibernéticas" (De Vergara y Trama, 2017) el cual describe los aspectos que se desarrollan en el espacio cibernético y como todas esas acciones afectan al componente de la defensa del poder nacional desde distintas perspectivas. "La estrategia de Argentina y Brasil para la defensa Cibernética, un análisis por los niveles de la Conducción" (Cabral, 2015) este documento realiza una apreciación general con respecto a cómo Argentina y Brasil emplean las nuevas tecnologías en materia de Ciberdefensa. "Empleo de las redes informáticas en Ciberoperaciones en el marco de la Gran Unidad de Batalla" (Cabrera, 2019). El presente trabajo busca estandarizar el empleo de las redes informáticas en operaciones dentro de una Gran Unidad de Batalla (GUB) a través de ejemplos históricos marcando la relevancia actual de las Ciberoperaciones. "La conducción de operaciones de Ciberdefensa: principios básicos en el campo de combate moderno" (Anca, 2015), se analiza el Ciberespacio y las acciones que se ejecutan en él, determinando los principios que aplica el comandante para la conducción de este tipo de operaciones. "La Ciberguerra como amenaza de los Sistemas de defensa integrados

y basados en redes del Teatro de Operaciones" (Miranda, 2014) desarrolla las medidas necesarias para incrementar la capacidad de Ciberdefensa en las redes, determinando la formación necesaria del personal a integrar una organización que se encargue de proteger dichas redes especificando las vulnerabilidades del sistema.

Relacionado con el estado actual de la cuestión, en referencia a los trabajos y bibliografías del párrafo anterior, estas enfocan el tema desde distintas perspectivas y niveles, pero en ninguno se detalla específicamente qué y cuáles son los procesos de trabajo que permitan el desarrollo de Operaciones de Ciberdefensa en el nivel Componente Terrestre, cómo el elemento que las llevará a cabo en este nivel de la conducción o la estructura de la cadena de comando que dirigirá el planeamiento y ejecución así como el control de las mismas.

Objetivos

Para responder al problema de estudio y en consonancia con lo expresado en la justificación del mismo, se ha propuesto como objetivo general:

Determinar el proceso de trabajo y el elemento que permita concretarlo dentro del Componente Terrestre del Teatro de Operaciones, para llevar a cabo Operaciones de Ciberdefensa.

En este sentido, se fijaron metas intermedias que permitirán arribar a conclusiones parciales que contribuirán al objetivo general; y siguiendo una secuencia lógica de razonamientos, estas se materializaran en tres objetivos particulares:

1) **Objetivo particular 1:**

Analizar el marco legal para el empleo del Ciberespacio como parte del Ambiente Operacional, y para determinar limitaciones y responsabilidades dentro del CTTO.

2) **Objetivo particular 2:**

Determinar las principales amenazas y objetivos/infraestructuras críticas militares para determinar las capacidades en Ciberdefensa que deberá contar el Elemento en apoyo.

3) Objetivo particular 3:

Integrar el análisis del marco legal junto con las amenazas dentro del CTTO para determinar el elemento y sus procesos de trabajo que permitan desarrollar Operaciones de Ciberdefensa.

Metodología a Emplear

El método a emplear para la confección del presente trabajo será el deductivo, planteando como punto de partida un objetivo de carácter general desprendiéndose de este, objetivos particulares con sus respectivas conclusiones parciales que responderán a cada uno de ellos. Posteriormente se arribara a conclusiones finales de carácter general que tendrán la intención de dar respuesta al objetivo general planteado en el presente trabajo. El diseño de este trabajo será del tipo explicativo, empleando como técnica de validación el análisis bibliográfico, documental y lógico.

Capítulo 1

El Marco Legal y empleo del Ciberespacio.

La finalidad del presente capítulo es determinar cuáles son las limitaciones que impone y las responsabilidades que le asignan a las Fuerzas Terrestres (FFTT) para la ejecución de Operaciones de Ciberdefensa a fin de asegurar el empleo y control del Ciberespacio. Tratando de expresar, a través de las conclusiones, cuales son las actividades que deben estar en capacidad de realizar el Instrumento Militar Terrestre y cuáles no, debiendo determinar el temperamento a seguir.

Esto genera la necesidad de contar con políticas y directivas claras que posibiliten desalentar amenazas en este ámbito, pudiendo tomar el ejemplo de otros Estados o la comunidad internacional; en donde se trabaja de manera combinada e interagencial.

Marco Legal Nacional

Cómo mencionaremos, la aparición de este nuevo domino, ha fijado al instrumento de la defensa nuevas responsabilidades y limitaciones en su empleo. El deber del Estado Nacional es asegurar mediante sus distintos componentes la seguridad e integridad territorial detectando las posibles amenazas neutralizándolas a través de una fuerza que genere una capacidad de disuasión creíble. Una de las características del Ciberespacio, a diferencia de otros dominios, es que no posee fronteras definidas y el origen de las posibles amenazas es muy amplio y variado.

La rápida y constante evolución de este ámbito y las tecnologías que operan en él, necesita de un marco normativo dinámico que pueda cambiar y actualizarse rápidamente para adaptarse y prevenir las nuevas y futuras amenazas. Estos cambios se pueden ver reflejado con más notoriedad en el plano internacional.

El marco legal Nacional ha evolucionado en forma contradictoria como causa de sus continuos cambios, falta de coordinación y la ausencia de constancia/proyección en el tiempo

respecto a las políticas de Defensa y el empleo de sus FFAA. Como ejemplo de esto se puede remitir a los continuos cambios de dirección en lo dispuesto en la Directiva de Política de Defensa Nacional, en donde en el año 2018 se adoptó una nueva concepción de los conflictos modernos; en donde el Ciberespacio toma mayor relevancia dentro del desarrollo de las operaciones y lo identifica como un nuevo domino así como los actores, regulares e irregulares, que pueden actuar en él son tenidos en cuenta como parte de los conflictos, independientemente de su naturaleza. Esto marca una diferencia significativa con las Directivas anteriores; aunque actualmente debido al cambio de gobierno en el año 2019, se volvió a lo establecido en la anterior DPDN de año 2014. Y posteriormente como desarrollaremos más adelante, es nuevamente modificada en el año 2021 limitando el accionar de las FFAA al origen o naturaleza de la amenaza.

Ley Nro 23.554 de Defensa Nacional

Comenzando con el análisis del marco legal, se desarrollará como pilar la Ley de Defensa Nacional Nro 23.554, sancionada y promulgada en el año 1.988. A través de ésta, se buscó garantizar la soberanía e independencia de la Nación Argentina, su integridad territorial y capacidad de autodeterminación; protegiendo la vida y la libertad de sus habitantes (Congreso de la Nación, 1988).

En su Título I° enuncia los principios básicos; el Artículo 1° expresa que se busca establecer en la presente ley haciendo referencia a las bases jurídicas, orgánicas y funcionales fundamentales para la preparación, ejecución y control de la Defensa Nacional (Congreso de la Nación, 1988).

En su Artículo 2° establece que es la Defensa Nacional y quienes la ejercen, resaltando que solo atañe a los conflictos que requieran el empleo de las Fuerzas Armadas, de forma disuasiva o efectiva, y aquí marca una limitación; que será solo ante agresiones de origen externo (Congreso de la Nación, 1988). Y determina también cual es la finalidad del empleo de las

fuerzas. Expresando en su Artículo 3° como se concreta la Defensa Nacional a través de un conjunto de planes y acciones.

Esta ley en su Artículo 4°, se considera relacionado con el Artículo 2°, en donde se resalta la importancia de diferenciar la Defensa Nacional de la Seguridad Interior, para la cual existe una ley particular. Aquí vuelve a remarcar la naturaleza externa de las agresiones y la limitación de las fuerzas armadas de accionar en el propio territorio independientemente del origen de las agresiones y su grado de afectación de la Seguridad Nacional. En relación con el tema de investigación y las limitaciones que impone dicha ley, no se podrían ejecutar acciones de Ciberdefensa ante una agresión de origen interno.

En relación con este punto el contenido de la Ley de Seguridad Interior Nro 24.059, del año 1991 y promulgada en 1992, establece en su artículo 27°, título V° De la complementación de otros organismos del Estado, que a requerimiento del Comité de Crisis las Fuerzas Armadas podrán apoyar operaciones de Seguridad Interior mediante el empleo de los servicios de Arsenales, Intendencia, Sanidad, Veterinaria, Construcciones y Transporte como así también de elementos de Ingenieros y/o Comunicaciones, contando con un representante del Estado Mayor Conjunto (Congreso de la Nación, 1991).

Posteriormente sus artículos 28° y 29° establecen los lineamentos del accionar en caso de un atentando a una jurisdicción militar en tiempo de paz; fijando cuales son las responsabilidades y quién debe responder a esa agresión, estableciendo por un lado que vulnera la Seguridad Interior y por otro fija como obligación de la autoridad militar la preservación de la fuerza y el restablecimiento del orden interno de dicha jurisdicción. Particularmente en el artículo 28° establece que las autoridades constitucionales mantendrán plena vigencia de sus atribuciones salvo la aplicación del artículo 6° (Congreso de la Nación, 1988).

Dentro de la misma ley, relacionado con el empleo de elementos de la Defensa Nacional en temas de Seguridad Interior y sus actividades correspondientes, enuncia en los artículos 31°

y 32°, título VI° Empleo Subsidiario de elementos de combate de las Fuerzas Armadas en operaciones de Seguridad Interior (Congreso de la Nación, 1992), la prerrogativa del empleo de las fuerzas armadas para el restablecimiento de la Seguridad Interior en territorio nacional, resaltando esta situación como de extrema gravedad, mediante el establecimiento del estado de sitio dictado por Congreso Nacional o el Presidente de la Nación en caso de que el 1ro no se encuentre en funciones, quien deberá designar un comandante operacional; permitiendo así el empleo de elementos de combate para reestablecer la situación de seguridad. De acuerdo a lo descripto anteriormente y excepcionalmente, ante esta situación las Fuerzas Armadas podrán ejecutar operaciones de Ciberdefensa en el marco interno pero atendiendo a una finalidad diferente.

Continuando con el análisis esta ley, en su artículo 5° establece los espacios en los cuales se podrán emplear los elementos que componen las Fuerzas Armadas nombrando a los espacios continentales, Islas Malvinas, Georgias del Sur y Sándwich del Sur y demás espacios insulares, marítimos y aéreos de la República Argentina, así como el sector Antártico Argentino, con los alcances asignados por las normas internacionales y los tratados suscriptos o a suscribir por la Nación esto sin perjuicio de lo dispuesto por el artículo 28° en cuanto a las atribuciones que dispone el Presidente de la Nación para establecer teatros de operaciones para casos de la guerra o conflicto armado (Congreso de la Nación, 1988). Como se puede observar en este artículo, el mismo no contempla al Ciberespacio como parte de un Teatro de Operaciones, esto se debe a que esta Ley no ha sido actualizada desde su sanción en el año 1992.

La evolución tecnológica y la necesidad de transferencia de un gran volumen de información en forma rápida, hacen que este se conforme como una parte importante del ambiente operacional.

Por último, su artículo 30° establece que el Poder Ejecutivo Nacional, con aprobación del Congreso Nacional, podrá declarar Zona Militar a los ámbitos, que por resultar de interés

para la Defensa Nacional, deban ser sometidos a la custodia y protección militar (Congreso de la Nación, 1988); entendiendo que de cumplir lo descripto en este artículo en referencia al Ciberespacio permitiría el llevar a cabo las operaciones de Ciberdefensa necesarias ante amenazas externas sin la necesidad de la configuración de un teatro de operaciones.

Directiva de Política de Defensa Nacional

Prosiguiendo con el marco legal, se procederá a analizar la Directiva de Política de Defensa Nacional (DPDN), sancionada en el año 2021 mediante el decreto 457/2021. Inicialmente teniendo en cuenta las Directivas de Política de la Defensa Nacional (DPDN) anteriores, en lo que son consecuentes es la relevancia de contar con elementos especializados a nivel conjunto y especifico que posean las capacidades necesarias para proteger la información y asegurar el empleo del Ciberespacio confiablemente.

La DPDN 2021, realiza una apreciación global que sirve como marco de referencia para la política de Defensa Nacional de la República Argentina, a continuación, se describen y analizan los escenarios mundial y regional, a los efectos de identificar tendencias para la formulación y permanente actualización de la política jurisdiccional.

La política de Defensa Nacional se desarrolla de manera articulada y complementaria con la política exterior, buscando contribuir de este modo a la protección de los intereses vitales y estratégicos de la Nación, a la consolidación de la paz regional y a la vigencia del derecho internacional (Ministerio de Defensa, 2021). A través de una apreciación estratégica global busca establecer lo que llama tableros estratégicos para poder comprender el marco internacional actual y a futuro para determinar su incidencia en el país y en sus Fuerzas Armadas. Como resultado de esta apreciación marca tres tableros; los centros de poder, los cuales describe en su texto, el estratégico-militar, el económico-comercial y el de las relaciones transnacionales.

En relación y de incumbencia para el desarrollo del trabajo, son de mayor interés el estratégico-militar y el transnacional. Referido al primero; establece una evolución a nivel global, con la supremacía de EEUU como única potencia mundial y su incremento en el gasto militar produciendo una brecha tecnológica. En este campo los usos militares de las tecnologías han llevado a la modificación de la profesión y técnicas militares en el empleo de sistemas de armas modificando el campo de batalla. Este proceso descripto, marca el documento, ha generado una tendencia hacia ubicar nuevamente las tensiones y conflictos de naturaleza interestatal. Esto puede interpretarse como un cambio en lo que se denominó Guerra contra el Terrorismo, corriéndola del centro de escena, retornando nuevamente a conflictos interestatales, marcando tendencia y el condicionamiento para el empleo de las acciones de Ciberdefensa como parte de las operaciones militares solo ante agresiones de origen externo de Fuerzas Militares, y consecuentemente restringiendo a su planeamiento.

Por otro lado describe el tablero transnacional; en el cual esgrime que se puede observar una dispersión del poder como consecuencia de la multiplicidad de actores. Aquí aborda el tema del aumento de la capacidad en la transmisión de datos y su relación con las nuevas tecnologías contemplando la aparición de nuevas vulnerabilidades y la disputa del control de los medios de transmisión y almacenamiento, entre estados-empresas privadas; remarcado la importancia de la Ciberdefensa ante estos nuevos hechos y analizando prospectivamente como crucial los posibles nuevos escenarios como la defensa del Ciberespacio. Este ámbito ha generado replanteos sobre las tradicionales categorías con las que se abordaba la “guerra real”, exigiendo una rápida adaptación por parte de los sistemas de defensa (Ministerio de Defensa, 2019).

En las últimas décadas, muchos países han reorientado sus esfuerzos y recursos para resguardar su ámbito ciberespacial; considera como principal característica que no constituye un espacio en sí mismo sino como una dimensión que cruza transversalmente a los dominios

ya conocidos, pero admite que si bien las acciones en el Ciberespacio son de naturaleza virtual pueden tener un impacto en el mundo físico (Ministerio de Defensa, 2019). Este riesgo se puede ver plasmado a nivel mundial a través de las potencias, las que han actualizado sus políticas de defensa y modernizado sus fuerzas para poder operar en este campo. La apreciación sobre la virtualidad que marca en las operaciones, se ve refutada en ejemplos históricos en los cuales se requiere de una operación complementaria para concretarla; como ejemplo al querer implantar un malware en una red informática cerrada necesariamente se deberá infiltrar personal para su concreción.

En su capítulo II°, concepción y posicionamiento estratégico de la República Argentina en materia de defensa, establece los objetivos que persigue. Define una estrategia defensiva que limita el accionar de todo el Instrumento Militar, el que debe contar con un nivel de disuasión creíble para desalentar intenciones externas. Además, contempla resguardar los recursos de valor estratégicos como medulares en la formación y preparación de esta actitud estratégica. Relacionado con estos objetivos contempla como factor complementario a las Tecnologías de la Información y Comunicación (TIC) como contribuyentes al progreso y desarrollo, destacando como aspecto importante resguardar el entorno digital relacionado con el empleo del Ciberespacio.

Asimismo, el decreto establece que el resguardo soberano debe garantizarse sobre la infraestructura de las TIC localizadas en el territorio nacional. Bajo esta conceptualización, la Ciberdefensa debe minimizar el riesgo de la exposición y contrarrestar eventos que afecten la libre disponibilidad del Ciberespacio en las operaciones militares que realice el Instrumento Militar, en cumplimiento de la normativa vigente en materia de Defensa Nacional (Ministerio de Defensa, 2021); aquí contempla al Ciberespacio, militarmente hablando, como parte del ambiente operacional en el cual se configuran amenazas para el desarrollo de las operaciones

militares, así como también a las tecnologías que contribuyen con los objetivos de valor estratégico comprendidos en la Directiva, pero a la vez restringe su accionar al desarrollo de operaciones de disuasión o preventivas y defensivas contemplando como posibles agresores a otros estados y no a entes no gubernamentales.

El capítulo III°, en sus instrucciones al Ministerio de Defensa, establece que se deben desarrollar todos aquellos aspectos concernientes a la política de Ciberdefensa en el nuevo ciclo de planeamiento de la Defensa Nacional. Adoptar las medidas necesarias para el fortalecimiento del sistema de Ciberdefensa desde los organismos conjuntos hasta los específicos de cada fuerza y determina el objetivo operacional del sistema. Coloca al sistema de Ciberdefensa como una de las prioridades en la Defensa Nacional y establece los lineamientos al Estado Mayor para incrementar la capacitación del personal en este ámbito. Establece como responsabilidad este orientar y coordinar los proyectos tendientes a lograr una arquitectura única de comando y control en el Nivel Estratégico Militar, que resulte interoperable e integrable con todos los niveles de la conducción Nivel Estratégico Nacional, Nivel Estratégico Militar, Nivel Estratégico-Operacional y Nivel Táctico (Ministerio de defensa, 2021).

Lo desarrollado precedentemente en el párrafo anterior marca un creciente reconocimiento e interés por parte de las autoridades políticas en la importancia del control, prevención y acción ante amenazas en el Ciberespacio. En concordancia con esto, las fuerzas armadas ya se encontraban bajo un proceso de gestión ante este tipo de amenazas mediante la creación en el año 2014 del Comando Conjunto de Ciberdefensa y posteriormente de los elementos específicos de cada Fuerza trabajando en forma coordinada con otras instituciones del estado para mitigar el impacto en los objetivos estratégicos nacionales.

Ley Nro 25.520 de Inteligencia Nacional

La inteligencia también tiene responsabilidad en la ejecución de actividades de en el Ciberespacio con la finalidad principal de obtener información, que será de utilidad para los elementos que deban ejecutar acciones miliares de Ciberdefensa.

Sancionada y promulgada en el año 2001, tiene por finalidad regular todas las actividades del Sistema de Inteligencia Nacional; "dentro de las cuales establece que sus actividades consisten en la obtención, reunión, sistematización y análisis de la información referida a los hechos, riesgos y conflictos que afecte las Defensa Nacional y Seguridad Interior" (Congreso de la Nación, 2015).

En su artículo 5° establece que:

> Las comunicaciones telefónicas, postales, de telégrafo o facsímil o cualquier otro sistema de envío de objetos o transmisión de imágenes, voces o paquetes de datos, así como cualquier tipo de información, archivos, registros y/o documentos privados o de entrada o lectura no autorizada o no accesible al público, son inviolables en todo el ámbito de la República Argentina, excepto cuando mediare orden o dispensa judicial en sentido contrario (Congreso de la Nación, 2001, p. título II).

Lo descripto en el párrafo anterior, tiene estrecha relación con lo que es transmitido a través del Ciberespacio y su seguridad, lo cual es una de las actividades que compete y de las que se ocupa la Ciberdefensa pero impediría realizar algún tipo de operación sobre ella.

Política de Ciberdefensa

Esta resolución y su anexo fijan lineamientos en los más altos niveles de la conducción los cuales repercuten en los niveles más bajos. En el año 2019 se dicta la resolución Nro 1380/19 del Ministerio de Defensa, estableciendo la definición de Ciberdefensa adoptada por el Estado Nacional y su política de defensa en torno a ella. Consta de seis artículos, particularmente en el artículo 3° y su correspondiente anexo fija la política en cuestión.

En su artículo 1° establece como definición de ciberdefensa:

> Entiéndase por CIBERDEFENSA a las acciones y capacidades desarrolladas por el Ministerio de Defensa, el EMCO y las Fuerzas Armadas para anticipar y prevenir ciberataques y ciberexplotación de las redes nacionales que puedan afectar al Ministerio de Defensa y al Instrumento Militar de la Defensa Nacional, como así también a las Infraestructuras Críticas operacionales soporte de los Servicios Esenciales de interés para la Defensa o a Infraestructuras operacionales soporte de procesos industriales de fabricación de bienes sensibles para la Defensa o que posibiliten el acceso a los activos digitales estratégicos adjudicados a su custodia."(Ministerio de Defensa, 2019, p. 5).

Esta definición solo prevé capacidades para anticipar y prevenir, haciendo a un lado aquellas actividades mediante las cuales se efectué algún tipo de respuesta ante la amenaza o agresión.

Enuncia en su artículo 3°:

> Apruébese la Política de Ciberdefensa consistente en CUATRO (4) Líneas de Acción principales que se desarrollarán conjugando TRES (3) ejes de políticas y cuya implementación se realiza a través de DOS (2) planes en orden de cumplimentar los objetivos aprobados por el artículo 2º del Decreto Nº 684 del 3 de octubre de 2019, descriptos en los Anexos I (IF-2019-96170351-APN-SSC#MD), II (IF-2019-96170945-APN-SSC#MD), III (IF-2019-96171204-APN-SSC#MD), IV (IF-2019-96172220-APN-SSC#MD) y V (IF-2019-96171563-APN-SSC#MD), los que se acompañan a la presente Resolución (Ministerio de defensa, 2019, p. 5).

En su anexo 4° especifica:

> A partir de conceptualizar al ciberespacio como un espacio soberano y la misión encomendada al Ministerio de Defensa de anticipar y prevenir ciberataques que pudieran comprometer la disponibilidad de los sistemas y redes de la Defensa, se han dispuesto

> acciones para fortalecer las capacidades de vigilancia y control en orden a cumplimentar los objetivos que se incorporan en PLANILLA ANEXA (Ministerio de defensa, 2019, pp. 5-6).

De la lectura de la resolución y su anexo, se pueden destacar los siguientes aspectos: el establecimiento de una política para el desarrollo de capacidades para la interacción en el Ciberespacio, la protección del mismo como espacio soberano, el establecimiento de un plan para la adecuación de las organizaciones militares y el plan de adecuación de infraestructuras críticas de la Defensa Nacional.

Resolución Nro 1523/2019 – Glosario de Ciberseguridad

Sancionada en el año 2019 por la Jefatura de Gabinete de Ministros (Secretaría de Modernización), esta resolución establece una serie de definiciones estandarizando conceptos relacionados con la Ciberdefensa. Se encuentra compuesta por dos anexos, en su Anexo II fija el concepto de Ciberespacio como el entorno complejo que resulta de la interacción de personas, software y servicios de internet a través de dispositivos y redes conectados, no posee existencia física sino que es un dominio virtual que engloba todos los sistemas TIC (Secretaría de Modernización, 2019). Este documento no brinda una definición de Ciberdefensa como tampoco considera una existencia física del Ciberespacio como parte del ambiente operacional. Una definición importante que presenta de interés para el trabajo se encuentra presente en su Anexo I, relacionada las Infraestructuras Criticas (IICC):

> 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 (Ministerio de Modernización, 2019, p. 1).

En este párrafo hace referencia a las infraestructuras de la Defensa. También define las IICC de la información y los criterios que identifican a estas, dentro de esto marca el impacto en el ejercicio de las funciones del Estado siendo de particular interés la defensa.

Resolución 343/14 del Ministerio de Defensa.

Esta resolución crea el Comando Conjunto de Ciberdefensa en el año 2014, bajo la dependencia directa del EMCO en la cual establece su misión:

> "Realizar la conducción de operaciones de Ciberdefensa, de manera permanente, con el fin de garantizar las operaciones militares del Instrumento Militar de Defensa Nacional, en cumplimiento de su misión principal y de acuerdo con los lineamientos establecidos en la planificación estratégica militar" (Ministerio de Defensa, 2014, p. 1).

Un importante aspecto de esta resolución es que reconoce al Ciberespacio como una dimensión operativa transversal a los otros dominios operativos tradicionales, en donde son desarrolladas operaciones de carácter militar, la que requiere una planificación militar particular.

Marco Internacional

Manual Tallin

En referencia al marco internacional, existente acuerdos, convenios y/o tratados, que al analizarlos nos permiten contar con una visión más amplia sobre el tema en cuestión y ver como es abordado por otros estados.

En el cuaderno de Estrategia N° 149 del Instituto Español de Estudios estratégicos, establece que:

> Que la Alianza Atlántica, fuera la primera en percibir la necesidad de acomodar las respuestas tradicionales al nuevo escenario estratégico, está inmersa en un proceso de transformación profunda de sus estructuras, procedimientos y capacidades, con el fin

> de conseguir unas fuerzas aliadas mejor dotadas, interoperables y capaces de actuar con la máxima eficacia.
>
> Los ataques cibernéticos ya no solamente tienen motivación intelectual o económica, sino también política, por lo que las consecuencias ya no sólo se centran en una pérdida económica, sino en los conflictos entre países que demuestran y miden sus fuerzas, además de en las dimensiones de tierra, mar, aire y espacio, a través del ciberespacio"(Durán, 2010, pp. 220-221).

En el año 2013 es creado por un grupo de expertos de la OTAN, el Manual de Tallin 1.0 como consecuencia de los ataques cibernéticos sufridos por Estonia que afectaron su infraestructura critica. Este manual busca regular a nivel internacional la ley de Ciberseguridad y la parte cibernética de los conflictos armados relacionando las consecuencias que pueden provocar las Ciberoperaciones, tanto lesiones físicas o muerte a personas o daños a objetos con el jus ad bellum (el derecho sobre el empleo de la fuerza) y jus in bello (el derecho a la guerra). Este manual es actualizado en el año 2017 a su versión 2.0, en el cual se realiza un análisis mucho más completo sobre la legislación vigente de las operaciones en el Ciberespacio anexando, como elemento extra, un análisis del marco jurídico sobre incidentes comunes y por los que no es necesario desatar un conflicto armado o el empleo de la fuerza.

Conclusiones parciales

Luego del análisis de los diferentes documentos que componen el marco legal existente y actual en la República Argentina, junto a una breve cita y descripción del ámbito internacional, se pudo arribar a las siguientes conclusiones parciales que serán de utilidad para continuar con el desarrollo de la investigación y poder contribuir a estructurar los procesos de trabajo que desarrollen las operaciones de Ciberdefensa en el nivel táctico.

- Los constantes cambios en el plexo normativo de la República Argentina, principalmente en la Directiva de Políticas de Defensa Nacional, producto de las distintas visiones políticas, de las administraciones, relacionadas a la Defensa, han provocado un retraso en el desarrollo de doctrina conjunta y específica, así como en la conformación de una estructura como así en la obtención y/o actualización del equipamiento de la fuerza, el cual no condice o se efectúa en simultaneo con la evolución tecnológica de las operaciones de Ciberdefensa.
- La división entre la Seguridad Interior y la Defensa Nacional obliga a que la Ciberseguridad y la Ciberdefensa sean llevadas a cabo por distintos organismos gubernamentales, estableciendo que la segunda se ocupe de asuntos de naturaleza militar exterior, aunque igualmente deba acatar y respetar normas de la Secretaría de Modernización y su comité de Ciberseguridad.
- El desfasaje temporal de la Ley de Defensa Nacional con respecto a la evolución de los conflictos y las tecnologías tiene como consecuencia la no contemplación del Ciberespacio como parte del ambiente operacional del Teatro de Operaciones en contrapartida con lo detallado en la Directiva de Política de Defensa Nacional del año 2021. Debería actualizarse la Ley a fin de aunar conceptos y contemplar las condiciones actuales.
- La nueva Directiva de Política de Defensa Nacional del año 2021 hace especial hincapié en el desarrollo de organismos conjuntos y específicos en materia de Ciberdefensa a través de la dirección del Comando Conjunto de Ciberdefensa, el cual debe normar las actividades

para toda la fuerza. Esta consideración debería dar paso al desarrollo de doctrina conjunta que siente las bases establecer las normas generales y permita la confección en el marco específico de la doctrina necesaria para hacer frente a las amenazas y su aporte particular al concepto sistémico de Defensa.

- La Ley de Defensa Nacional complementada por la Directiva de Política de Defensa Nacional, limita el empleo del Instrumente Militar Terrestre, ya que este solo puede accionar ante agresiones de origen extranjero de fuerzas militares de otros estados. En relación a este aspecto señalado, es importante para ser tenido en cuenta, que determinar el origen de la agresión cibernética es de difícil por lo que requerirán de un trabajo interagencial con las Fuerzas de Seguridad o Policiales y demás organismos gubernamentales que tengan injerencia en este ámbito para poder dar una respuesta satisfactoria ante estas amenazas. Ambas, Ley y directiva, prevén una actitud netamente defensiva del Instrumento Militar, esto limita el accionar ofensivo y/o exploratorio mediante, que permitan constituir una respuesta más rápidas y efectivas para neutralizar preventivamente amenazas potenciales o reales capaces de afectar los propios sistemas y consecuentemente los intereses de la Nación.
- La consolidación del ciberespacio como un nuevo elemento del ambiente operacional, hace necesario que el Estado Nacional brinde a sus Fuerzas Armadas las herramientas legales para que estas puedan accionar en forma rápida y precisa ante las amenazas contra la Defensa Nacional, buscando protegerlas y minimizar su impacto.
- El estudio detallado en el Manual del Tallin proporciona importantes precedentes en materia internacional para alcanzar un consenso sobre definiciones legales relacionadas al Ciberespacio y las acciones que se ejecutan en él. Esto permitirá unificar normativas del Derecho Internacional entre Estados favoreciendo la cooperación. La inserción de la Argentina mediante la adhesión a convenios internacionales y regionales en materia de Ciberseguridad y

Ciberdefensa beneficiaran la integración, el desarrollo tecnológico, la actualización de procedimientos de Defensa no solo contra agresiones interestatales sino intraestatales.

Capítulo 2

Determinar las principales IICC Militares a ser afectadas por las operaciones de Ciberdefensa dentro del CTTO.

La intención de este capítulo es poder identificar aquellas amenazas reales o potenciales que permitan definir cuáles podrían ser los posibles objetivos que busque afectar el enemigo y que comprometan el correcto funcionamiento de los distintos sistemas y subsistemas que apoyan la conducción de las operaciones militares dentro del Componente Terrestre del Teatro de Operaciones. Es preciso comprender y definir algunos conceptos como Ciberespacio, Ciberdefensa, IICC, amenaza para luego interrelacionándolos poder llegar a las conclusiones parciales del capítulo.

Para el desarrollo de una operación militar debe ser necesario definir el ambiente operacional en el cual se desarrollarán. En el reglamento para la Conducción de las Fuerzas Terrestres, lo define como:

> Conjunto de factores de diversa naturaleza que existen en forma estable y semiestable en una determinada región. Ellos influirán en la determinación de la composición, magnitud, equipamiento y aptitud de las Fuerzas que en él deban intervenir, como así también en la aplicación de su poder de combate. Lo conforman la influencia de la política y la estrategia nacional y militar, el ambiente geográfico, los factores militares, las características de la lucha, los sistemas de armas que pueden emplearse, factores sociales, los medios de información y su influencia en la opinión pública (Ejército Argentino, 2015, p.30).

Este amiente operacional se deberá analizar sistémicamente en cuanto a sus componentes, los cuales están interrelacionados, esto implica un análisis desde múltiples puntos de vista para obtener una visión más amplia y objetiva.

Por su parte el General Brett Williams, Director de Operaciones del US CyberCommand en The Joint Force Commander's Guide to Cyberspace Operations, esgrime que:

> Si se concentra la atención en el nivel operacional de la guerra, se encuentra que las operaciones en el espacio cibernético son bastante similares a las operaciones que se llevan a cabo en los otros ámbitos. El espacio cibernético es un espacio operacional, como es el mar, el aire, la tierra y el espacio (p.14).

Por lo tanto, de acuerdo a lo expuesto precedentemente, cuando se refiere a las operaciones militares relacionadas a las Ciberdefensa, el entorno o ambiente operacional se denominara Ciberespacio.

Ciberespacio

El Ciberespacio es un entorno de carácter global que evoluciona constantemente, en este ambiente las amenazas son cada vez más activas y sofisticadas por la naturaleza de los actores que actúan en él, estas amenazas pueden poner en riesgo no solo las redes y sistemas de información, inteligencia o comunicaciones de las Fuerzas Armadas sino también las IICC del instrumento militar que afecten la conducción de las operaciones. Se debe pensar en él integralmente teniendo en cuenta todas sus capas y componentes. Es un ámbito tanto físico como virtual en donde se desarrollaran actividades de todo tipo a través de redes, software, hardware y firmware de dispositivos electrónicos. Exige una integración con el resto de los actores dentro del Teatro de Operaciones.

Como se mencionó y describió en el capítulo anterior, dentro de la Resolución 1523/19, no se contempla al Ciberespacio como un dominio físico sino solamente virtual. Por su parte Daniel Kuhel define al ciberespacio como:

> El conjunto de dominio global dentro del entorno de la información cuyo carácter único y distintivo viene dado por el uso de la electrónica y el espectro electromagnético para

> crear, almacenar, modificar, intercambiar y explotar información a través de redes interdependientes e interconectadas utilizando las tecnologías de información y comunicaciones (Kuehl, 2009).

Este autor lo considera un nuevo dominio y a su vez nombra otros componentes que no son tenidos en cuenta.

En cuanto al reglamento de terminología castrense, solo en el de carácter conjunto, se define al Ciberespacio como: "ámbito virtual en el que se desarrollan actividades de procesamiento, almacenamiento y explotación relacionadas con los datos e información digital, a través de redes interdependientes e interconectadas, software, firmware de dispositivos, cuyo carácter distintivo está dado por el empleo de las tecnologías de la información y la comunicación" (EMCO, 2015)**.** En cuanto a la doctrina brasileña de Ciberdefensa, dentro del MD31M-07 se refiere al Ciberespacio como el espacio virtual compuesto por dispositivos de computación conectados o no a redes, donde la información digital transita y se procesa y/o almacena (p.18). Cuando se habla de Ciberespacio por lo general se lo relaciona a un entorno virtual donde solo interactúan operadores de equipos informáticos a través de la red.

Hoy en día las operaciones en el Ciberespacio han evolucionado utilizando tropas en la capa física. Ejemplo de esto fue el control de Urketelecom por parte de las tropas rusas en Crimea en el año 2014 o la instalación de un virus en la planta nuclear de Nataz en Irán a través de un dispositivo USB. Dentro de la doctrina del Ejercito de los Estados Unidos establecen una relación y dependencia del Ciberespacio con los dominios físicos terrestre, aéreo y marítimo.

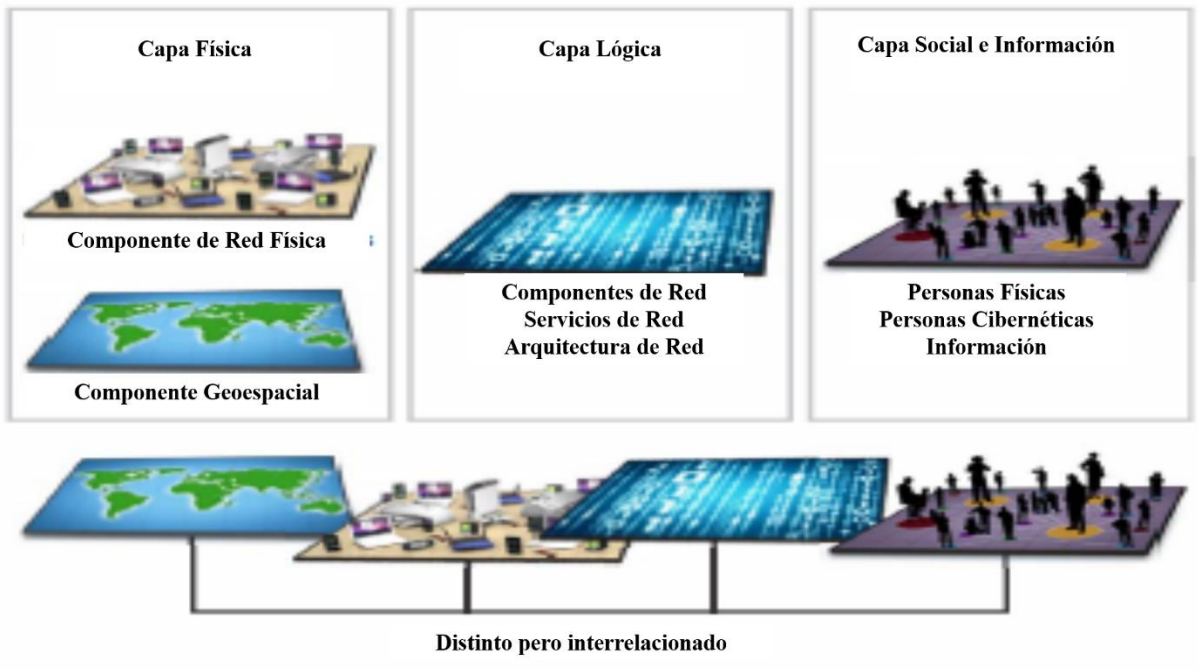
Habiendo citado distintas fuentes para observar los diferentes conceptos sobre el Ciberespacio, podemos asegurar que a similitud de los otros dominios tiene características particulares que afectarán al nivel táctico, en donde operan actores de variada naturaleza. En relación a este tema, según el reglamento del Ejército de los Estados Unidos de Norteamérica JP 3-12 Cyberspace Operations de junio 2018 (p.I-3), el Ciberespacio es un ámbito operativo dentro

del instrumento militar y del Componente Terrestre; y se encuentra conformado por las siguientes capas:

- Capa Física, es el medio a través del cual se desplazan los datos. Está integrada por los componentes geoespacial que se refiere a la ubicación en la tierra, aire o mar en donde se encuentren las redes. Los componentes de la red física son hardware, software e infraestructura (cables, sistemas inalámbricos, enlaces electromagnéticos, satélites y enlaces ópticos) que soportan las redes y conectores físicos (cables, radiofrecuencia, enrutadores, conmutadores, servidores y computadoras).
- Capa Lógica. Compuesta por aplicaciones de red, componentes de servicios de red y componentes de arquitectura de red.
- Capa Social e información, compuesta por personas físicas como componente, el componente de ciber persona y los componente de información.

Figura 1

Estructura del Ciberespacio



Nota. Adaptación y traducción propia. El grafico representa las diferentes capas que componen al ciberespacio. Tomado de Cyberspace Operations JP 3-12 (p.I-3), por KEVIN D. SCOTT Vice Admiral, USN Director Joint Force Development, 2018, US Army.

Ciberdefensa

Luego de haber descripto y conceptualizado el Ciberespacio, describiendo sus características particulares, en los párrafos precedentes, dan marco para continuar desarrollando el Capítulo considerando como otro aspecto importante a definir la Ciberdefensa. Teniendo como base lo que se expresa en los manuales militares, para poder determinar si existe un concepto uniforme en cuanto a su definición y en base a ella poder observar cuales son las posibles amenazas que pueden configurarse. Según la terminología conjunta, es: "Conjunto de acciones desarrolladas en el Ciberespacio de interés del sistema de defensa para prevenir y/o contrarrestar toda amenaza o agresión cibernética" (EMCO, 2015, p.42). De acuerdo a la doctrina específica del Ejército Argentino es una Operación complementaria y entiende que son el conjunto

de acciones que se desarrollan en el Ciberespacio con la intención de prevenir, detectar, identificar, anular, contener o repeler las amenazas o agresiones cibernéticas (Ejército Argentino, 2015).

Establece como producto del proceso de globalización, entiéndase empleo de sistemas y redes de TIC, se incorpora al Ciberespacio o espacio cibernético como nuevo ambiente operacional. Este nuevo ambiente, a diferencia de los ya conocidos que poseen limites definidos, abarca a los otros y los integra virtualmente mediante sistemas materiales o físicos factibles de ser destruidos por medios convencionales. También establece que:" este ambiente es virtual, no reconoce fronteras locales o interestatales, ni es posible tampoco ejercer sobre él un grado de control definido y conocido", aclara que es difícil distinguir con claridad al agresor al igual que sus fines en concordancia con lo descripto en el marco legal, en cuanto a quien deberá actuar ante determinada amenaza u agresión.

El creciente empleo de los sistemas y redes informáticas, para la transmisión de información, se constituye como objeto de amenazas en este ambiente particular; por lo que será necesario contar con personal instruido y material adecuado para operar a través del Ciberespacio asegurando lo propio y dificultando o afectando a lo del enemigo. También específica y asigna un grado de responsabilidad a cada elemento del Componente Terrestre que emplee o forme parte de estos sistemas o redes en el cumplimiento de normas y procedimientos para asegurar el normal funcionamiento y el control del Ciberespacio de interés (Ejército Argentino, 2015).

Para la doctrina militar brasileña, el concepto de Ciberdefensa establecido en el MD31-M-07 de 2014; la contempla como el conjunto de acciones ofensivas, defensivas y exploratorias que se llevan a cabo en el ciberespacio, en el contexto de una planificación nacional coordinada, de nivel estratégico e integrada por el Ministerio de Defensa, con el propósito de proteger los

sistemas de información de interés para la Defensa Nacional, obteniendo datos para la producción de inteligencia y comprometer los sistemas de información del oponente (p.18).

Al no contar con doctrina específica referida a Ciberdefensa, en ninguno de los niveles de la conducción, tomaremos en base a los conceptos expuestos precedentemente que la Ciberdefensa implica la planificación y ejecución de operaciones militares, defensivas u ofensivas y de explotación o inteligencia en el Ciberespacio tendientes a proteger los sistemas y redes. Las formas de acción de la Ciberdefensa pueden variar de acuerdo con el nivel en que se empleen, la tecnología con la que se cuente, el tiempo para su planificación y despliegue.

En nuestro reglamento de Conceptos básicos sobre Sistemas de Comunicaciones, Informática y Guerra Electrónica de la Fuerza, establece que el apoyo de comunicaciones e informática se materializa, en parte, por la instalación, operación y mantenimiento de redes informáticas integradas y que son parte del Ciberespacio en donde se desarrollan las operaciones de Ciberdefensa. A su vez, a través de estas redes se ejecutan las operaciones de Ciberdefensa por lo cual se necesita esencialmente de las actividades y tareas de seguridad informática como componente principal de estas operaciones. Esta seguridad informática, que contribuye a la Ciberdefensa, se considera como un componente primario y esencial para organizar el sistema; este tipo de seguridad se proporciona a través de la protección física de los sistemas de campaña de enlaces y bases de datos o servidores de las redes. Una protección lógica a través de software para poder acceder a la red y antivirus o malware; y una protección de empleo lograda mediante el estricto cumplimento de las directivas-normas-procedimientos operativos que se dicten (Ejército Argentino, 2016, p.CapVII-19).

Operaciones Militares en el Ciberespacio

En los conceptos descriptos en el párrafo anterior, referido a la Ciberdefensa, alude a acciones netamente del ámbito militar. Estas acciones, se materializan mediante la ejecución

de operaciones militares en el Ciberespacio u operaciones de Ciberdefensa, de acuerdo al origen de la doctrina. Estas deberán potenciar las capacidades militares para poder efectuar una respuesta oportuna en el Ciberespacio ante amenazas o agresiones que puedan afectar los Sistemas del Componente Terrestre.

Para la Junta Interamericana de Defensa (2020), define a las operaciones en el Ciberespacio de la siguiente forma: "las ciberoperaciones son acciones militares planificadas, organizadas, coordinadas y llevadas a cabo por unidades de Ciberdefensa con la finalidad de lograr efectos en el ciberespacio, así como en los otros ámbitos de operaciones" (p.42). Con estas operaciones se busca prevenir, preservar y contrarrestar toda amenaza en el Ciberespacio que intente afectar a las IICC de la información dentro del TO. Se planifican y ejecutan en forma contribuyente con el resto de las operaciones.

Cuando hablamos de Ciberdefensa y sus operaciones en el nivel Táctico, y haciendo la analogía con la definición enunciada en la página 15, referido a las IICC y que se entiende por ellas, trasladándolo al ámbito militar y en particular a este nivel se materializan en infraestructuras criticas militares del instrumento militar (IICCMM). Para su correcta identificación, no es tan relevante la infraestructura en sí, sino la función que cumple o el servicio que presta. Aquellas funciones que proveen un servicio al instrumento militar, como el comando y control-vigilancia-inteligencia-comunicaciones-sostén logístico, se las debe considerar esenciales para el desarrollo de operaciones; porque su funcionamiento es indispensable y no permite alternativa de reemplazo, por lo que su afectación o destrucción tendrá un impacto negativo sobre las operaciones militares o el normal funcionamiento de los sistemas.

De acuerdo a lo expresado por De Vergara y Trama (2017), para Francia las operaciones en el espacio cibernético incluyen acciones defensivas (lucha informática defensiva LID), las acciones de exploración (exploración informática, IE) y las acciones ofensivas (lucha informá-

tica ofensiva, LIO). Todas ellas son conducidas por la cadena de comando operacional de defensa cibernética. Para el Reino Unido las operaciones cibernéticas son la planificación y sincronización de actividades en y a través del espacio cibernético para permitir la libertad de maniobra y, de esa manera, alcanzar los objetivos militares. Pueden categorizarse en cuatro funciones distintas: las operaciones cibernéticas defensivas (DCO[1]); las operaciones cibernéticas ofensivas (OCO[2]); las operaciones de ciberinteligencia, vigilancia y reconocimiento (IVR[3]); y las operaciones cibernéticas de preparación operacional del ambiente (p.49).

La "Doutrina Militar de Defesa Cibernética" de Brasil, al igual que la de España y Francia clasifican a las operaciones cibernéticas solamente en ofensivas, de protección y de exploración (p.51). Según la Guía de Ciberdefensa de la Junta Interamericana de Defensa establece que las Ciberoperaciones son de seis tipos, Ciberoperaciones Defensivas pasivas y activas, Ciberoperaciones de explotación pasiva y activa; Ciberoperaciones de respuesta u ofensivas todas referidas en la Figura 2 (pp. 42-43). De acuerdo expresa la doctrina Norteamericana en su publicación conjunta 3-12 establece como operaciones militares en el Ciberespacio a las operaciones defensivas en el Ciberespacio, operaciones ofensivas en el Ciberespacio (p. II.3).

[1] DCO: Defensive Ciberoperations
[2] OCO: Offensive CIberoperations
[3] IVR: Intelligence, vigilance and reconnaissence

Figura 2

Ciberoperaciones

Nota. Tomado de Guía de Ciberdefensa (p. 42), por Junta Interamericana de Defensa, 2020, Copyright © 2020 Junta Interamericana de Defensa.

Luego de un análisis basado en fuentes extrajeras, principalmente, podemos establecer, en particular para este trabajo, que el tipo de Operaciones de Ciberdefensa son tres tipos: las Operaciones Ofensivas, Defensivas y de Exploración de acuerdo a la finalidad que persiguen y los efectos que busquen materializar.

Las operaciones ofensivas de Ciberdefensa son aquellas acciones que se ejecutan buscando interrumpir, negar el acceso o destruir información o los sistemas informáticos que se encuentran almacenados en los dispositivos que lo componen y en las redes informáticas y de comunicaciones del enemigo, su concreción se llevará a cabo a través de diferentes acciones que permitan cumplir el efecto buscado. Las operaciones defensivas de Ciberdefensa se desarrollan en forma simultánea y coordinada por los elementos de Ciberdefensa y de Seguridad informática buscando neutralizar ataques y explotación cibernética contra nuestros dispositivos, IICCMM, redes informáticas y de comunicaciones mediante el incremento de acciones de seguridad, defensa y guerra cibernética; son actividades de carácter permanente y que al igual

que las ofensivas comprenden acciones que conllevan a lograr efectos. Por ultimo las operaciones de exploración o ciberinteligencia serán aquellas que buscarán o recolectarán datos o información de los Sistemas Informáticos de interés para obtener un conocimiento detallado del enemigo y propio. Estas acciones deberán evitar ser rastreadas y contribuir a identificar las vulnerabilidades de los sistemas de ambos oponentes.

Por otra parte, un aspecto importante a tener en cuenta, dentro de la doctrina del Ejército de Estados Unidos y que también marcan De Vergara y Trama (2017) son las denominadas Actividades cibernéticas y electromagnéticas (CEMA) que integran y coordina las actividades en el ciberespacio con las electromagnéticas en razón de que el dominio en el que actúan cada una tienen áreas de desempeño comunes y se representan en la Figura Nro 3. Con este tipo de actividades consiguen obtener sinergia en los efectos de ambos dominios, coordinando los medios humanos y materiales (p.229). Esto se debe a que los elementos que operan en el ciberespacio están conectados y son apoyados por estructuras físicas, sistemas electrónicos que operan en una porción del espectro electromagnético (EEM) para lograr una mayor capacidad de transferencia de información a mayor velocidad. El manual M3-38 conceptualiza al CEMA como:

> Actividades que buscan como objetivo explotar las ventajas sobre el enemigo en el espacio cibernético y en el espectro electromagnético a la vez que, de forma simultánea, le deniega su uso y protege al sistema de mando y control de la misión (US Army, 2014, p. 1-1).

Figura 3

Funciones interrelacionadas de la ejecución de las actividades de CEMA en el espectro electromagnético y el ciberespacio.

Nota. Tomado de OPERACIONES MILITARES CIBERNÉTICAS (p. 228), por G. A. Trama, Gustavo Adolfo y E. A. de Vergara, 2017, Escuela Superior de Guerra Conjunta de las Fuerzas Armadas.

Ciberamenzas

En el Ciberespacio en general al igual que el nivel táctico, no es la excepción, existen numerosos y diversas tipos de amenaza cada vez más sofisticadas, con distintos niveles de impacto de acuerdo a la finalidad que persigue sobre el objetivo, esto requerirá por parte del agredido escoger una determinada medida particular al momento de seleccionar la acción defensiva que permita anular, bloquear o impedir la afectación de nuestro sistema.

Según la terminología castrense conjunta se entiende por amenaza a la acción consciente y deliberada de un actor que, teniendo capacidad, muestra la intención o da indicio de probable concreción de un perjuicio en contra de los propios intereses (EMCO, 2015). Las ciberamenzas se constituyen como potenciales fuentes, externa o interna, que buscarán afectar,

de distintas formas, a los sistemas de la organización a través de las operaciones en el Ciberespacio; esta aprovechará cualquier vulnerabilidad detectada en sus componentes, humano o tecnológico, buscando afectar en objetivos de mayor valor. Para que una fuente sea considerada una ciberamenza deberá encontrarse en capacidad de ejecutar esa acción y contar con intención de ejecutarla como describe el concepto de amenaza. Para identificar la ciberamenza se deberá determinar la fuente, de donde proviene y luego seleccionar de las posibles fuentes cual está en capacidad de ejecutarla.

Los posibles objetivos de interés para las ciberamenazas son la información disponible en los dispositivos que componen las redes informáticas, las redes en sí, los dispositivos móviles de comunicación y los distintos tipos de sistemas que componen el instrumento militar terrestre. Cuando hablamos de ciberamenzas en el nivel táctico, estas buscarán afectar aquellos sistemas como los de Comando y Control, de Armas, de Control, de Comunicaciones y Computarizados. En la actualidad en consonancia con el desarrollo tecnológico dentro del campo de combate, se busca tener sistemas que permitan transmitir en forma casi inmediata y en gran volumen información para lo toma de decisiones; como ejemplo podemos citar al Sistema Integrado Táctico de Comando y Control del Ejército Argentino (SITEA).

Según el reglamento de Conceptos Básicos de Comunicaciones, Informática y Guerra Electrónica los sistemas de comando y control independientemente del nivel de conducción que se trate y de la magnitud de las fuerzas al que se aplican, son una conceptualización sobre las “herramientas” que necesita el comandante/jefe y su estado mayor/plana mayor, para ejercer la conducción de las fuerzas a su disposición y hacerlo en forma eficiente, como condición “sine qua non” para obtener la victoria o alcanzar los objetivos, dependiendo de la operación militar que se trate. El Ejército Argentino adopta “conceptualmente” la sigla de C3 I2, este es un conjunto de medios humanos, equipos y materiales de alta tecnología (p.I-5).

El SITEA integra bajo un mismo sistema a los elementos de comando, de maniobra, apoyo de fuego, apoyo de combate y logísticos. Esta herramienta permite integrar los Puestos Comandos a través de los medios de comunicaciones con capacidad para transmitir voz y datos en forma segura y recibir información captada por otros medios (sensores, radares, satélites, GS, elementos de exploración, etc.). El SITEA está compuesto por componentes tecnológicos, procedimientos y sistemas de información (hardware, software, redes, equipos de telecomunicaciones, etc.) (Ejército Argentino, 2020).

Otro ejemplo de estos sistemas es el Sistemas Automatizado de Tiro de Artillería de Campaña (SATAC) que busca mejorar e incrementar las capacidades de los Grupos de Artillería de Campaña mediante el procesamientos de la información de los diferentes subsistemas del arma para reducir los tiempos de análisis y ejecución de las misiones de fuego (Ejército Argentino, 2020), este sistema a similitud del anterior también emplea los medios de comunicaciones para su funcionamiento.

La relación entre los sistemas descriptos previamente y el tema abordado en el capítulo, es que son sumamente vulnerables a las acciones del enemigo como parte de las operaciones de Ciberdefensa. Igualmente para citar otro ejemplo, que buscarán afectar las ciberamenazas, podemos nombrar los Sistemas de Comunicaciones; los cuales pueden ser afectados por operaciones que no sean de naturaleza cibernética, pero afectarán a los medios que permiten el tráfico de información que circula a través del Ciberespacio. Este tipo de operaciones, sabotaje-golpes de mano-espionaje etc., afectando los medios de comunicaciones como el Terminal Satelital de Campaña Remolcable (TSCR), Radioenlace Digital de Campaña (RDC) u otros equipos que forman parte de las redes informáticas, contribuirán a completar o complementar la finalidad de las operaciones de Ciberdefensa.

Conclusiones parciales

En consideración al tema desarrollado en este capítulo, en el que se buscó poder conocer las distintas y posibles ciberamenazas que se pueden configurar dentro del Teatro de Operaciones; a través de las que se puedan adoptar las medidas preventivas que correspondan a fin de lograr proteger las infraestructuras críticas militares (IICCMM) y asegurar el comando y control de las operaciones, es que se ha llegado a las siguientes conclusiones.

Mediante un análisis, profundo y detallado, sobre las capacidades del enemigo, teniendo como base la información que se disponga previamente sobre equipamiento, procedimientos, grado de instrucción, capacidades y su actualización constantemente; se podrá llegar a determinar las posibles ciberamenazas que se presenten en este ámbito del Teatro de Operaciones y a su vez establecer cuáles serán las IICCMM a afectar. Por ello, el comandante deberá contar con medidas preventivas en busca de contar con un Ciberespacio operacional seguro y confiable.

Para la ejecución de operaciones de Ciberdefensa, en el Teatro de Operaciones, se complementará con la previa ejecución de operaciones de exploración del Ciberespacio para obtener información sobre las vulnerabilidades del o los objetivos que se buscará defender o atacar. Estas operaciones deben evitar ser rastreadas pero al mismo tiempo permitir obtener información. A su vez estas operaciones, como en todos los niveles, deberán estar sincronizadas y coordinadas con el resto de las operaciones militares que se ejecuten en el resto de los dominios para contribuir a lograr los objetivos asignados.

En la Argentina, se adopta según fijan las normas del marco legal, una actitud defensiva en todos los ámbitos pero no se deberá descuidar la capacidad para poder ejecutar operaciones ofensivas de Ciberdefensa mediante la preparación de técnicas, métodos y capacidades del personal y material como parte de las operaciones planteadas en la dinámica de la defensa, al igual que estipulan nuestros reglamentos para los medios de las diferentes armas.

Por otra parte luego del análisis desarrollado en el capítulo, referido al Ciberespacio y las acciones de Ciberdefensa en el teatro de operaciones; se deduce que es muy difícil lograr determinar su origen, como también su naturaleza y poder establecer los límites correspondientes al mismo a diferencia de los otros dominios. Debido a esto es responsabilidad del Comandante, determinar para cada fase cuáles serán las IICCMM a proteger y los efectos cibernéticos necesarios que contribuyan al logro de la maniobra operacional, del nivel táctico. Esto se logrará mediante el desarrollo de capacidades en Ciberdefensa y contar con superioridad tecnológica para contar con libertad de acción mediante el seguro y confiable empleo del Ciberespacio.

En relación a lo desarrollado en el párrafo anterior y entendiendo que solo se permite realizar operaciones de tipo defensivas, en el caso de poder identificar el origen y naturaleza de la agresión, y que esta sea interna o no de naturaleza militar se deberá contar con una relación y comunicación interagencial estrecha entre las FFAA y de Seguridad, forjada desde la paz, que permita al elemento que corresponda actuar llevando a cabo las acciones que sean necesarias. Por otra parte, en el caso de que la naturaleza del incidente sea externo pero no militar, debería existir una excepción dentro del marco legal que le permita al Componente Terrestre poder actuar ante esta situación.

Capítulo 3

Determinar los procesos de trabajo y el elemento que ejecute las Operaciones de Ciberdefensa.

En el presente capítulo tendrá la finalidad de determinar, genéricamente, cuáles podrían ser los procesos de trabajo que permitan desarrollar aquellas operaciones de Ciberdefensa, para asegurar el comando y control de las operaciones y el funcionamiento de los distintos subsistemas.

Proceso de Trabajo

Para iniciar con el desarrollo del capítulo se remitirá fuera del ámbito militar algunas de las conceptualizaciones que se utilizan para definir a los procesos de trabajo. Como ejemplos podemos citar los siguientes; un conjunto de relaciones que se establecen entre el hombre, los objetos y medios de trabajo; con el propósito que los objetos sean transformados y que se conviertan en un producto final (Quiroa, 2020). Otra conceptualización los define como una secuencia de tareas que se realizan de forma concatenada, es decir de forma seguida una detrás de la otra para alcanzar un objetivo o un fin concreto. En una organización, la suma de muchos procesos tendrá como resultado la entrega de un producto o servicio al cliente (Torres, 2020).

Para el presente trabajo de investigación se entenderá por proceso de trabajo a una secuencia de tareas y actividades que se realizan en forma concatenada y secuencial para alcanzar un objetivo o fin concreto, en particular incluirán a las actividades de planeamiento y posterior ejecución que permitan llevar a cabo las operaciones de Ciberdefensa, en todos sus tipos y dentro del Teatro de Operaciones.

En relación a esta definición nuestro manual de Conducción de las FFTT al igual que el de Terminología castrense específico y conjunto establecen al planeamiento como el conjunto de actividades destinadas a establecer objetivos, determinar políticas o modos de acción

y preparar los planes correspondientes; comprendiendo la identificación y definición del problema, reunión, organización y procesamiento de información, la apreciación de situación, desarrollo de los modos de acción, adoptar resoluciones y preparar los planes y/o órdenes (Ejército Argentino, 2015); esta definición es similar y guarda relación con la de proceso de trabajo.

El trabajo se focaliza en tratar de establecer un posible proceso de planeamiento, el cual se desarrollara mediante una serie de actividades particulares, para operaciones de Ciberdefensa y que permita su posterior ejecución; determinando también las actividades que conlleva, en forma coordinada y eficiente que contribuye al planeamiento y ejecución de la operación principal.

El planeamiento es una de las actividades básicas de la conducción, a través del Proceso de Planificación de Comando (PPC) nos permitirá arribar a una solución de un Problema Militar Operativo (PMO) el cual está caracterizado por la oposición inteligente del enemigo (Ejército Argentino, 1998). Este proceso lógico nos permitirá enfrentar una situación de incertidumbre, evitando aplicar un proceso de prueba y error. De acuerdo a la naturaleza del problema necesita un planeamiento de iguales características que contribuya a llegar a una solución mejor.

Planeamiento de las Operaciones de Ciberdefensa

Como se mencionó en los antecedentes, actualmente nuestra doctrina específica o conjunta sobre Ciberdefensa, se encuentra en desarrollo en consecuencia no hay muchos aspectos doctrinarios vigentes. Sin embargo se han encontrado en algunos reglamentos conceptos que se refieren al tema, citando como un ejemplo a lo descripto en el manual de Conducción de las FFTT que establece:

> "Los aspectos relacionados con el planeamiento y ejecución de operaciones de defensa cibernética serán establecidos en los reglamentos funcionales de las organizaciones militares con responsabilidad primaria en la materia. No obstante,

> y desde el nivel operacional hacia los menores niveles, la totalidad de los comandantes o jefes y sus órganos de asesoramiento y asistencia deberán considerar, en forma permanente, los riesgos existentes para el desarrollo de otras operaciones en caso de que sus Fuerzas sean blanco de ataques cibernéticos. Asimismo, deberán adiestrar a sus Fuerzas para (además de saber combatir con los sistemas informáticos existentes) operar con procedimientos manuales alternativos en caso de que los sistemas informáticos en uso hayan sido afectados. Un aspecto prioritario para incluir en los planes será la elaboración de normas y procedimientos de seguridad informática, relacionadas con el empleo de sistemas con posibilidad de transmisión de datos, incluyendo sistemas de control de tiro, sistemas de vigilancia electrónica, de comunicaciones, de comando y control y medios de comunicación personales los que incluyen telefonía celular de todos los integrantes de la Fuerzas" (Ejército Argentino, 2015, p. CAP VII-55).

En el plano internacional, se enuncia en la Guía de Ciberdefensa, como cualquier otro tipo de unidad militar que ejecute operaciones de otra naturaleza debe contar con un grupo de personas con conocimientos particulares en aspectos operativos fundamentales en ciberdefensa agrupados dentro de un elemento de comando teniendo como responsabilidad de asesorar para la toma de decisiones en esta área en particular; este elemento de asesoramiento desarrollara los planes específicos. El planeamieno de las Operaciones de Ciberdefensa se debe realizar mediante una secuencia lógica y estándar para que facilite el apoyo a operaciones de otra naturaleza y su integración (p.52-53).

Para la Junta Interamericana de Defensa, el planeamiento de las Operaciones de Ciberdefensa se basa en tres fases; la identificación de las ciberamenazas mediante el análisis de los cuatro casos generales (amenaza y respuesta conocidas; amenaza conocida y respuesta desconocida; amenaza desconocida y respuesta conocida; y amenaza y respuesta desconocidas) para

luego identificar y clasificar las amenazas más probables y más peligrosas; estableciendo sus formas de actuar y sus potenciales impactos, establecer soluciones. Identificación de funciones críticas, aquellos servicios, funciones, sistemas que de ser interrumpidos puede provocar el mal funcionamiento de la organización y establecer mediciones del impacto para provocar una respuesta. Por último la fase de definición de medidas de Ciberdefensa en la que se describen todas las medidas de prevención y reacción necesarias para recuperarse de los impactos previstos, como reaccionar ante los imprevistos y prevenir las amenazas desconocidas (p. 53-54)

Teniendo presente la aplicación del arte y diseño de las operaciones, el elemento encargado de la Ciberdefensa deberá realizar un proceso de planificación específico para las operaciones en este ámbito del ambiente operacional, contribuyendo al logro del efecto o los efectos perseguidos a través del Ciberespacio, como por ejemplo el ciclo de toma de decisiones del enemigo. Dentro del planeamiento uno de los aspectos de mayor relevancia a determinar, serán las IICCMM. Para ello es preciso que cuente dentro de su orgánica con un elemento a fin, el cual se hará mención posteriormente dentro del capítulo. Este elemento deberá, dentro de sus capacidades, estar en condiciones de poder realizar el proceso de planificación en forma sincrónica, integrada y coordinada con el elemento al que apoya. Para identificar este proceso se denominará Planeamiento de Operaciones de Ciberdefensa (POC).

Para su desarrollo, dentro del Nivel CTTO, se seguirá la siguiente secuencia:

Como primer paso, se deberá identificar el problema en cuestión mediante un análisis detallado de la misión, identificación de los recursos disponibles para lograr los efectos requeridos y a proteger, análisis del Ciberespacio de interés, limitaciones impuestas por el escalón superior o que sean enunciadas producto del análisis, que atañen al empleo o ejecución de las operaciones en el Ciberespacio; identificación de las IICCMM (objetivos) propias y del

enemigo en nuestra zona, que afecten el funcionamiento sistémico como también el cumplimiento del efecto; requerimientos de información necesarios, las tareas que se deriven del estudio inicial.

Continuando con este proceso, como segundo paso, se deberá establecer las posibles capacidades de Ciberdefensa del enemigo en base al análisis previo de las IICCMM a afectar por él, y elaboración de los modos de acción de Ciberdefensa los que deben cumplir el análisis de la prueba de aptitud, factibilidad y aceptabilidad. Una vez definidos estos aspectos permitirá comenzar a esbozar requerimientos y exigencias para el diseño del Sistema de Ciberdefensa.

En el tercer paso se desarrollará una confrontación con el apoyo de un software que permita la simulación de los modos de acción definidos en el paso anterior, observando en que porcentaje permiten cumplimentar los efectos propios sobre los sistemas del enemigo, los elementos necesarios intervinientes y/o a disposición (nivel superior); obtener un resultado posible que permita generar un programa de control para poder adoptar aquellas previsiones necesarias para dar respuestas alternativas que permitan la adaptación de nuestro sistema para enfrentar eventualidades. Mediante este paso se logrará determinar cuál de los modos de acción confrontados es mejor. Posteriormente dentro del paso se efectuará una comparación mediante un análisis de las diferentes posibles soluciones, realizando un estudio de las ventajas y desventajas de cada modo de acción; a través de esta comparación se arribará al mejor modo de acción de Ciberdefensa que permita concretar los efectos solicitados. De ser necesario se podrán esbozar conclusiones respecto al modo de acción seleccionado para apoyar la operación.

Para finalizar este proceso, en el cuarto paso, se materializa la resolución del responsable de Ciberdefensa y el diseño del concepto de apoyo al Plan en todas sus fases que permitirán el desarrollo de las Operaciones de Ciberdefensa, las que conformarán parte del Plan de Operaciones del Comandante del CTTO.

Formación en Ciberdefensa

Como aspecto importante se debe dar prioridad en su educación a los Oficiales y Suboficiales de la institución, ya que son la columna vertebral de la organización. Siempre con la finalidad de mejorar las competencias por medio de la formación superior profesional militar. En el presente dentro de la fuerza hay un solo elemento que tiene la misión y capacidades para desarrollar operaciones de Ciberdefensa; en el deberían estar destinados Oficiales y Suboficiales subalternos capacitados particularmente en el desarrollo de Operaciones en el Ciberespacio. Relacionado al tema en desarrollo, la Escuela de Comunicaciones ha comenzado a dictar un curso básico de Ciberdefensa para cuadros del Ejército, que busca trasmitir a los cursantes los conocimientos básicos generales sobre la materia y en la etapa planeamiento se encuentra uno avanzado.

Es relevante para el personal que deba realizar todos aquellos procesos que permitan concretar las operaciones de Ciberdefensa, recibir una formación profesional especial y permanente que le permita desarrollar las capacidades necesarias para hacer frente a la complejidad y evolución constante de las actividades en relación a este tipo de operaciones. Esta formación deberá contar con una parte individual y colectiva, como operador y a la vez como parte de una organización especializada en Ciberdefensa.

El adiestramiento del personal, al igual que en la ejecución de otro tipo de operaciones, se podrá perfeccionar mediante la ejecución de ejercicios de Ciberdefensa que incluyan aspectos técnicos y procedimentales mediante la ejecución de los tipos de operaciones descriptos en el capítulo anterior.

Los planes de la formación del personal deberán contemplar las actividades de concientización, formación y capacitación en Ciberdefensa en el marco de la legislación vigente.

Elemento de Ciberdefensa en el CTTO

El sistema de Ciberdefensa debería estar compuesto por diferentes organizaciones en apoyo a cada nivel de la conducción. En la actualidad en el Ejército el máximo elemento es la Dirección de Ciberdefensa, encargada de ejecutar las acciones Ciberdefensa como respuesta ante una amenaza con el fin de prevenir y preservar el empleo de las IICCMM y las IICCI del Ejército asegurando el Ciberespacio. El nivel táctico, particularmente en el CTTO, debería contar con un elemento en capacidad para coordinar, integrar y conducir operaciones de Ciberdefensa apoyando el desarrollo de las operaciones tácticas. Este elemento, independientemente de su magnitud, deberá estar organizado, equipado e instruido para instalar, operar y mantener el sistema de Ciberdefensa del Componente Terrestre. Dentro de su organización contará con un elemento de comando el cual este en capacidad de asistir y asesorar al jefe/comandante sobre las operaciones en este ámbito en particular, elaborar los planes, procedimientos, supervisar las operaciones de Ciberdefensa y establecer normas del elemento apoyado. También contar con un elemento logístico, el cual a través de la ejecución de las funciones y actividades logísticas permita el sostenimiento. Y contar dentro de su organización con un elemento específico, el cual tenga la responsabilidad de llevar a cabo cada tipo de operación particular de Ciberdefensa de las mencionadas en el capítulo 2; mediante la instalación, operación y mantenimiento de sus medios.

Conclusiones parciales

De acuerdo al objetivo particular del presente capítulo, su finalidad fue establecer el posible proceso de trabajo y el elemento que los realice para llevar a cabo las operaciones de Ciberdefensa en el marco del CTTO.

Se determina que es necesario en este nivel de la conducción contar por un lado con un elemento en apoyo al Componente Terrestre que se encuentre en capacidad para afrontar las exigencias que impone la explotación del Ciberespacio y poder asegurar la propia libertad de acción mediante un empleo seguro y confiable, permitiendo al Comandante contar con un comando y control eficiente de las operaciones. Se considera necesario que el elemento sea flexible de esta especificidad, cada uno de los elementos que conformen el subsistema particular de Ciberdefensa deberá conocer de forma clara sus objetivos, el efecto que se le requiere y las condiciones particulares para llevarlos a cabo

Simultáneamente para asegurar el empleo del Ciberespacio y la ejecución de operaciones de Ciberdefensa en sus diferentes modos, estas organizaciones deberán estar equipadas, instruidas y adiestradas para generar aquellas capacidades necesarias para realizar las operaciones necesarias. El personal que conforme estas organizaciones, deberá estar formado y capacitado específicamente en las técnicas particulares. Esta formación debe ser tanto técnica y como táctica para que le permita al individuo poder encontrar las soluciones técnicas necesarias a los problemas tácticos.

En el planeamiento se efectúa un previsión de empleo de los medios en base a la misión impuesta, mediante él se podrá detectar las falencias o faltantes de recursos permitiendo formular requerimientos necesarios al escalón superior. Por esto teniendo en cuenta la especificidad de las operaciones de Ciberdefensa y las particularidades del empleo del Ciberespacio, se necesitan procesos de trabajo particulares para realizar un planeamiento detallado mediante el

cual se obtengan resultados que permitan tomar mejores decisiones. Estos procesos de planeamiento buscarán disminuir la influencia de adoptar conclusiones en forma intuitiva. Este proceso no debe ser aislado sino guardar una estrecha relación y contribuir con el Proceso de Planeamiento de Comando.

Conclusiones Finales

En el desarrollo del presente trabajo se abordaron aspectos, considerados como base, para la determinación de un proceso de trabajo que permita mediante una secuencia lógica llevar a cabo las operaciones de Ciberdefensa en el nivel CTTO, esto motivó el desarrollo de tres objetivos particulares concatenados que dieron respuesta al general. En principio se realizó el análisis del marco legal normativo nacional y mencionando el internacional, basado en las leyes, decretos, normas, directivas y trabajos de investigación de la temática legal; tomando al Ciberespacio desde un enfoque que lo contempla para el empleo militar dentro del Teatro de Operaciones, de esta manera las operaciones que realicen los elementos de Ciberdefensa se encuentran dentro del marco legal Nacional estableciendo los límites de sus operaciones y permitiendo la defensa de las infraestructuras críticas de la información. Bajo las condiciones expuestas las acciones que lleve a cabo el enemigo la Ciberdefensa se encuentra en capacidad de actuar mitigando los daños, protegiendo las infraestructuras militares que puedan atentar contra los diferentes sistemas que permiten llevar adelante las operaciones. La doctrina militar deberá estar en concordancia con las necesidades operativas actuales producto de los constantes avances tecnológicos que impone la evolución de los medios que operan en el ciberespacio.

En primer lugar, teniendo como premisa que el marco legal debe ayudar al planeamieno de respuestas que sean eficaces y en tiempo real. Es necesario que las normas legales tengan continuidad en el tiempo y no imponer cambios drásticos en su orientación, ya que el desarrollo de la doctrina en el marco conjunto y específico estará basado en las directivas de defensa. Particularmente la Ley de Defensa Nacional, debería actualizarse a los parámetros actuales ya que data de un tiempo en que el Ciberespacio no había sido descubierto y empleado como un ambiente operacional para el desarrollo de operaciones militares. El desa-

rrollo de la doctrina sobre Ciberdefensa es una tarea dificultosa debido a la naturaleza compleja del ambiente, ya que simultáneamente se encuentra ubicada en tres capas y atraviesa los otros ámbitos y difícil de establecer límites o fronteras. Es por esto que debería adaptar el marco legal para que posibilite el desarrollo de operaciones ofensivas y proyectar poder en el Ciberespacio. Es necesario que las operaciones de Ciberdefensa se guíen por los mismos principios que el resto de las operaciones pero adaptados a sus particularidades que impone el ciberespacio.

En segundo lugar, se debe tener presente que las operaciones de Ciberdefensa es una opción más, que generara una capacidad especializada, con la que contará el comandante para contribuir a lograr los efectos necesarios para cumplir con su misión. Actualmente existe una dependencia creciente de los medios militares de las nuevas tecnologías que las convierte en un objetivo de la Ciberdefensa. Esta amenaza real obliga a contar con una capacidad de resiliencia real en Ciberdefensa que debe abarcar todos los medios considerados como infraestructuras críticas dentro del componente terrestre, esto exige el empleo seguro y confiable del Ciberespacio.

Otro aspecto importante para mitigar las amenazas, es la concientización del personal que debe traerse desde la paz, para evitar en campaña ser vulnerables a las operaciones de exploración de Ciberdefensa que son permanentes. El diseño actual, las redes que se emplean en campaña están conectadas a la red de uso diario en el Ejército Argentino, esto contribuye a la formación de la concientización de la seguridad en su empleo desde antes de entrar en operaciones. Actualmente la Ciberdefensa tiene un tinte diferente a las operaciones convencionales, ya que en este ámbito las operaciones del oponente son más rápidas, económicas, gozan de anonimato y posibilidad de ejecutarlas desde lugares fuera del Teatro de Operaciones o por actores no militares motivados por diferentes causas, es por esto la importancia de la concientización.

En general para que los ataques del oponente tengan éxito y logren afectar los propios sistemas se debe dar una falla en algún componente del sistema que puede vincularse a falta de concientización del personal en cuanto al empleo de los medios y redes informáticas; que el software que se emplee presente fallas de seguridad voluntarias o involuntarias, que la tecnología usada sea insuficiente o se encuentre desactualizada; ausencia de medidas concretas o que no sean cumplidas.

Relacionado con los ataques y su incidencia, los elementos de Ciberdefensa deben estar en condiciones de dar solución anticipada a estas agresiones, debiendo efectuar una preparación previa mediante la búsqueda e identificación, el análisis y posterior determinación de los riesgos que pueda causar un ataque (incidente, en el lenguaje de Ciberdefensa) sobre un objetivo o IICCMM de la información, para poder tomar acciones tendientes a reducir su impacto.

Una vez producido el ataque debe clasificarlo de acuerdo a su tipo a través de la detección y su análisis para poder determinar el procedimiento de respuesta. Consiguientemente llevar adelante las acciones planificadas para ese tipo de ataque. Este análisis permitirá conocer el entorno y los activos de información militar.

En tercer lugar, el cuadro que presentan las operaciones en este dominio supone una dinámica de trabajo particular. Los procesos de trabajo deben tender a prevenir las ciberagresiones que afecten las IICCMM del Componente Terrestre evitando que afecte los sistemas que lo componen. El personal especialista en operaciones de Ciberdefensa debe integrar el Estado/ Plana Mayor para asesorar o asistir en su área respectiva. Los temas desarrollados dentro de los capítulos 1 y 2 necesitan ser acompañadas por la capacitación progresiva del personal en todos los niveles.

La planificación de este tipo de operaciones requiere de coordinación de las capacidades del elemento de Ciberdefensa para lograr el/los objetivos y sincronizar los efectos que tienen

la finalidad de afectar y proteger en simultaneo. En la parte técnica se deben desarrollar sistemas operativos y programas propios tendientes a lograr una independencia y soberanía tecnológica.

Actualmente el dinamismo que caracteriza al combate moderno y consecuentemente al Ciberespacio, es necesario contar con un proceso de planeamiento particular que permita la modificación de los planes de las operaciones de Ciberdefensa en forma rápida y eficiente para adaptarse a la nueva situación impuesta por la constante recepción de información.

Para finalizar las conclusiones es importante considerar que para poder desarrollar la Ciberdefensa es necesario definir una doctrina específica que establezca las normas, los criterios y procedimientos particulares a seguir para el diseño, planeamiento y posterior ejecución de las operaciones a desarrollar en el Ciberespacio.

Como aporte profesional, tendiente a la necesidad de complementar el tema abordado y tomando de base lo desarrollado en la presente investigación, se propone que se investigue y evalué la posibilidad de crear dentro de las Unidades y Subunidades Independientes del Arma de Comunicaciones un elemento, de la magnitud adecuada y con las capacidades necesarias, para desarrollar el planeamiento y operaciones de Ciberdefensa en todas sus tipos y formas. Simultáneamente generar la doctrina específica de nuestra fuerza, para este nivel, en donde se detalle la organización y composición del Subsistema Particular de Ciberdefensa en el nivel táctico y su integración al Sistema Nacional, con la finalidad de estandarizar procedimientos para la concreción de este tipo de operaciones.

Este desarrollo debiera basarse en los productos que genere la nueva Directiva de Política de Defensa Nacional en el Ciclo de Planeamiento Estratégico Militar que comenzó este año. Esta propuesta se basa en la necesidad de contar con elementos de Ciberdefensa desplegables en el campo de combate para hacer frente a situaciones concretas.

Referencias

Aguirre Ponce, A.A. (2017). Ciberseguridad en Infraestructuras Críticas. Universidad de Buenos Aires.

Anca, L. J. (2015). La conducción de las operaciones de Ciberdefensa: Principios básicos en el campo de combate moderno. Escuela Superior de Guerra.

Azzolini, C.M. (2017). Ciberseguridad en la República Argentina y su perspectiva. Instituto de Inteligencia de las Fuerzas Armadas.

Baretto, J. F. (2017). La defensa nacional y la estrategia militar de seguridad cibernética. Escuela Superior de Guerra Conjunta.

Berett, W.T. (2014). The Joint Force Commander's Guide to Cyberspace Operations. Joint Force Quarterly 73, 2nd Quarter. http://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-73/jfq-73_12-19_Williams.pdf

Cabral Quiroz, V.J. (2015). La estrategia de Argentina y Brasil para la Defensa Cibernética, un análisis por los niveles de la conducción. Escuela Superior de Guerra.

Cabrera, C.I. (2019). Empleo de las redes informáticas en Ciberoperaciones en el marco de la Gran Unidad de Batalla. Escuela Superior de Guerra.

Decreto Nro 457/2021 (Ministerio de Defensa). Por la cual establece la Directiva de Política de Defensa Nacional. 14 de Julio de 2021.

Decreto Nro 571/2020. Modificación Decreto Nro 683/2018 y 703/2018. Boletín Oficial de la República Argentina.

Decreto Nro 703/2018 (Ministerio de Defensa). Por la cual se establece la Directiva de Política de Defensa Nacional. 31 de Julio de 2018.

Decreto Nro 2645 de 2014 (Ministerio de Defensa). Por el cual establece la Directiva de Política de defensa Nacional. 10 de Noviembre de 2009.

De Vergara, E y Trama, G. (2017). Operaciones Militares Cibernéticas – Planeamiento y Ejecución en el Nivel Operacional. Editorial Visión Conjunta.

Directiva del SUBJEMGE Nro 918/18. (Dirección General de Comunicaciones e Informática). Por la cual establece el régimen funcional del SUIE. 23 de noviembre 2018.

Directiva del SUBJEMGE Nro 829/21. (Dirección General de Comunicaciones e Informática). Por la cual se establece la Directiva Anual de Ciberdefensa. 05 Abril 2021.

Directiva del SUBJEMGE Nro 830/21. (Dirección General de Comunicaciones e Informática). Por la cual se establece la Directiva Anual de Comunicaciones e Informática.05 de Abril 2021.

Díaz del Río Durán, J.J. (2010). La Ciberseguridad en el ámbito militar. Instituto Español de Estudios estratégicos. Cuaderno de estrategia N° 149.

Ejército Argentino (1998). ROD-71-01-I Organización y Funcionamiento de los Estados Mayores – Tomo I. Dirección general de Organización y Doctrina.

Ejército Argentino. (2015). ROB-00-01 Conducción de las Fuerzas Terrestres. Dirección General de Organización y doctrina.

Ejército Argentino. (2016). ROD-05-01 Conceptos Básicos sobre Sistemas de Comunicaciones, Informática y Guerra Electrónica de la Fuerza. Dirección General de Organización y Doctrina.

Ejército Argentino. (2020). Sistema Integrado Táctico de Comando y Control del Ejército Argentino. Manual del Usuario. CIDESO.

Ejército Argentino. (2020). Sistema Automatizado de Tiro de Artillería de Campaña. Manual el Usuario. CIDESO.

Estado Mayor Conjunto (2014). PC-00-02 Glosario de Términos de Empleo Militar para la Acción Militar Conjunta. Estado Mayor Conjunto de las Fuerzas Armadas.

Estado Maior conjunto (2014) Doutrina Militar de Defesa Cibernética - MD31- M-07.1ª Edição /2014. Estado Maior conjunto das Forças Armadas..

Gago, E.A. (2017). El enfoque Argentino sobre Ciberseguridad y Ciberdefensa. Escuela Superior de Guerra.

Gamuzza, N. (2020). Guía de Ciberdefensa: orientación para el diseño, planeamiento, implantación y desarrollo de una ciberdefensa Militar. Junta Interamericana de Defensa.

Junta Interamericana de defensa (2020). Guía de Ciberdefensa. Orientaciones para el diseño, planeamiento, implantación y desarrollo de una ciberdefensa militar. Gobierno de Canadá.

Kuehl, Daniel (2009) "From Cyberspace to Cyberpower: Defining the Problem," en Franklin D. Kramer, Stuart Starr, y Larry K. Wentz (eds.), Cyberpower and National Security. National Defense UP.

Ley Nro 23554. Ley de Defensa Nacional. 13 de Abril de 1988.

Ley Nro 24059. Ley de Seguridad Interior. 18 de Diciembre de 1991.

Ley Nro 25520. Ley de Inteligencia Nacional. 27 de Noviembre de 2001.

Libro Blanco de la Defensa (Ministerio de Defensa). 01 de Septiembre de 2015.

Miranda, S.D. (2014). La Ciberguerra como amenaza a los Sistemas de Defensa integrados y basados en redes del Teatro de Operaciones. Escuela Superior de Guerra Conjunta.

Quiroa, M. (09 de Noviembre de 2020). Proceso de trabajo. https://economipedia.com/definiciones/proceso-de-trabajo.html

Resolución Nro 343 de 2014 (Ministerio de Defensa). Por la cual se establece la creación del CCCD). 14 de Mayo de 2014.

Resolución Nro 1380 de 2019 (Ministerio de Defensa). Por la cual se establece la definición de Ciberdefensa y la Política de Ciberdefensa. 25 de Octubre de 2019.

Resolución Nro 1523/2019 (Secretaría de Gobierno de Modernización). Por la cual establece la definición de Infraestructuras Críticas y de Infraestructuras Críticas de Información, la enumeración de los criterios de identificación y la determinación de los sectores alcanzados. 12 de Septiembre de 2019.

Sepetich, S.E. (2016). Las Ciberoperaciones aplicadas a un Teatro de Operaciones –Estudio de casos: Guerra Ruso Georgiana.

Torres, I. (Abril 2020). 15 Ejemplos de procesos de una empresa. https://iveconsultores.com/ejemplos-de-procesos-de-una-empresa/

United State of Defense (2018). JP 3-12 Cyberspace Operations. Joint Chiefs of Staff, Department of Defense.