
# MATERIA: TALLER DE TRABAJO FINAL INTEGRADOR

# TRABAJO FINAL INTEGRADOR

## TEMA:

La Ciberdefensa en el Nivel Operacional

## TÍTULO:

La identificación del Centro de Gravedad en las Ciberoperaciones en apoyo al Nivel Operacional

**PROFESOR:** DANISA RIERA.

**My CABRERA, Cristian Ivan**

**Año 2019**

**RESUMEN**

La falta de doctrina respecto a la ciberdefensa en el nivel operacional permite al adversario explotar esta vulnerabilidad para desarrollar operaciones de información que modelen la opinión pública. Aspecto que se agrava ante la complejidad del campo de combate moderno, donde los elementos del diseño operacional tienen un papel trascendental a la hora de concebir una campaña. Por tal razón, la determinación del centro de gravedad adquiere un rol determinante en el planeamiento, este proceso es responsabilidad del comandante del teatro de operaciones.

Dado que las ciberoperaciones puedan ser consideradas el centro de gravedad de una campaña y, que el nivel operacional aún no contempla al ciberespacio como un ambiente donde se desarrollan operaciones militares provoca un desafío cultural para las fuerzas armadas, donde la guerra centrada en redes soporta la capacidad de transformar la información en acción. Por ello, el objetivo general será identificar cuándo el centro de gravedad de las ciberoperaciones puede ser considerado el centro de gravedad de la campaña. Esto, se ejemplifica en los conflictos de Estonia 2007 o Ucrania 2014, donde se evidenció la importancia de las ciberoperaciones a la hora de desarrollar cualquier operación militar.

El centro de gravedad de las ciberoperaciones, dentro de la planificación de una campaña, busca generar efectos que impacten sobre la percepción de la población o el decisor y alteren el proceso de toma de decisiones en todo momento.

Con la ciberdefensa, los actores involucrados intentan producir el caos en el oponente y defenderse de estos ciberataques, para equilibrar el poder de combate tratando de obtener la victoria antes de desplegar su poder militar. De esta manera, se procura disminuir los daños colaterales que afecten sus relaciones internacionales y lo involucren en otros conflictos. Por lo desarrollado, se concluye que no hay un conflicto igual al otro, pero la fase de la campaña más propicia donde las ciberoperaciones buscaran afectar la percepción de la población y el proceso de toma de decisiones es la fase preparación. Por esto, el centro de gravedad de las ciberoperaciones en esta fase puede coincidir con el centro de gravedad de la campaña.

**Palabras clave.**

Ciberoperaciones, Ciberdefensa, Ciberseguridad, Ciberataque, Centro de Gravedad.

## TABLA DE CONTENIDOS

## ÍNDICE DE TABLAS

# INTRODUCCIÓN

El propósito del presente trabajo es determinar la eficacia de las ciberoperaciones durante el conflicto en el nivel operacional. Para lograrlo, la presente investigación abarca el desarrollo de los efectos que persiguen las ciberoperaciones ofensivas, defensivas, de exploración y de información en las redes que interactúan en el nivel operacional. Para ejemplificar esto, se tiene en cuenta el desarrollo de un conflicto moderno como Estonia 2007.

Las ciberoperaciones cambiaron el campo de batalla, la forma de luchar, los actores y los objetivos obligando a las Fuerzas Armadas del mundo a que actualicen su doctrina (Llongueras Vicente, 2013).

Por tal razón, el conflicto en Estonia que tuvo lugar en 2007 fue un hecho disruptivo de un ciberataque a gran escala. En él, la nación más digitalizada del mundo, Estonia, sufrió un ciberataque a sus infraestructuras críticas quedando paralizada por más de un mes (Gomez de Agreda, 2012).

Sin embargo, la OTAN dio a conocer al ciberespacio como un nuevo dominio de la guerra en la cumbre de Varsovia de 2016, nueve años más tarde del conflicto en Estonia (Moliner González, 2016). Además las Fuerzas Armadas más prestigiosos del mundo, al igual que diferentes células terroristas u otros organismos de influencia internacional, destinan importantes recursos personales y materiales para incrementar su influencia en el mundo complejo actual desde inicios del siglo XXI (Llongueras Vicente, 2013).

En lo que respecta a ciberseguridad, el trabajo se ajusta a lo desarrollado por Alejandro Corletti Estrada en sus obras *Ciberseguridad, una Estrategia Informático/Militar* y *Seguridad en Redes*. El autor desarrolla en esta bibliografía los términos de ciberseguridad, ciberresiliencia y ciberdefensa en profundidad (Corletti Estrada, 2017), (Corletti Estrada, A, 2016).

Para vincular la ciberdefensa con los elementos del diseño operacional de la campaña, se toman como fuente de investigación lo que marca la doctrina conjunta en el nivel operacional. Por esto, el análisis del centro de gravedad se evalúa de acuerdo a lo que desarrolla el planeamiento para la acción militar conjunta en el nivel operacional (PC20-01, 2017).

Estas ideas se complementan con lo desarrollado por Alejandro Kenny, Omar Locatelli y Leonardo Zarza en *Arte y diseño operacional*. En este texto, los autores abordan el planeamiento operacional y el estudio de los elementos del diseño operacional sobre diferentes ejemplos históricos de conflictos actuales (Kenny, Locatelli, Zarza, 2015).

No obstante, si bien el título de este TFI es de *La identificación del Centro de gravedad en las Ciberoperaciones en apoyo al Nivel Operacional*, existen en los antecedentes mencionados contenidos comunes que serán referidos en búsqueda de mayor profundidad y de acuerdo con el enfoque de esta investigación. En la actualidad, las Fuerzas Armadas de los países más desarrollados del mundo y los países emergentes se encuentran desarrollando la ciberdefensa en sus naciones para mejorar la protección de sus infraestructuras críticas y la información.

En la doctrina operacional de las Fuerzas Armadas argentinas no se menciona nada con respecto a la ciberdefensa en la actualidad. Por tal motivo, se la entiende como una responsabilidad de la estrategia nacional y militar, tanto en su planificación, como en su ejecución. Sin embargo, las potencias en ciberdefensa como Estados Unidos, Rusia, China o países emergentes de Latinoamérica como Brasil la vienen desarrollando desde los niveles tácticos. De esta manera, el dominio ciberespacial no reconoce jerarquías y solo posee lugar para aquellos que cuentan con el conocimiento para acceder a la información.

Por ello, en la era de la información, la digitalización de todos los sistemas de armas forma parte de Estados cuyas infraestructuras críticas[1] y servicios se vinculan permanentemente a las redes informáticas. Las naciones y las organizaciones interestatales posicionan al ciberespacio como un dominio preponderante para el desarrollo de la vida de las personas de una nación (Llongueras Vicente, 2013). En este dominio, interactúan los sistemas de armas de las Fuerzas Armadas, que el ciberterrorismo busca neutralizar a fin de dificultar la interoperabilidad de los sistemas y el comando y control de las operaciones.

La guerra en el ciberespacio es una guerra asimétrica. Los componentes de las fuerzas armadas y el nivel operacional deben trabajar para identificar las

[1] Son sistemas que se consideran esenciales y los servicios que prestan son vitales para las operaciones cotidianas, la economía, la seguridad y el bienestar general de las sociedades modernas". Así los define la Directiva europea: 2008/114/CE del 8 de diciembre de 2008.

vulnerabilidades de sus redes. Por esto, las ciberoperaciones se ejecutan con el empleo de fuerzas de dos o más agencias en acción coordinada para producir efectos deseados en apoyo a un objetivo común. De esta manera, es necesaria la cooperación del sector privado, ya que las principales vulnerabilidades en el ciberespacio se concentran en las empresas privadas.

Por esto, las operaciones basadas en efectos son fundamentales a la hora de establecer una línea de operaciones, ya que junto con la guerra en red fueron encumbradas como uno de los pilares de la transformación militar.

Esto está originando un cambio en la concepción del Instrumento Militar para los retos futuros, mediante el diseño de Fuerzas Armadas Conjuntas, organizadas en red, operando con efectos y combatiendo en toda la gama de operaciones. Esto deposita en las ciberoperaciones la necesidad de ofrecer una respuesta adecuada a los conflictos modernos actuales, que se amalgame con las nuevas amenazas del siglo XXI.

Sin embargo, en lo que respecta a ciberseguridad, los ciberguerreros deberán establecer políticas que permitan proteger sus redes e información vulnerable antes de recurrir a otras agencias. Esto permite, neutralizar el objetivo principal de la ciberguerra, que es el uso del ciberespacio para atacar infraestructuras, sistemas o equipamientos con la intención de limitar al oponente en la obtención información y proteger las capacidades propias (Llongueras Vicente, 2013).

Por todo lo expuesto, la identificación del centro de gravedad en las ciberoperaciones, de acuerdo con la fase de operación de la campaña, permitirá optimizar los recursos y mantener la libertad de acción e iniciativa de la operación en desarrollo. Las aseveraciones en el análisis y determinación del centro de gravedad de la doctrina en el nivel operacional de, *fuente de poder que proveen fortalezas o capacidades esenciales* (PC20-01, 2017) *y el ente primario que permite alcanzar el objetivo operacional* (Escuela Superior de Guerra Conjunta, 2015), *dan surgimiento al proceso investigativo: ¿Cuándo el centro de gravedad de las ciberoperaciones puede constituirse en el centro de gravedad de la campaña?.*

El campo de batalla moderno, enfrenta a dos oponentes que intentan doblegar su voluntad, con la particularidad que esta guerra se está librando en la mente de las personas por medio de ciberataques permanentes. Los ataques cibernéticos se

concentran en la explotación de las diferentes vulnerabilidades de un sistema o red de una manera no prevista, dando acceso al atacante y dificultando los procesos de toma de decisiones de su estructura de liderazgo.

Empero, estos ciberataques no solo provienen de fuera de los elementos de trabajo sino también de soldados o personal de trabajadores contratados que representan un riesgo (Ingeniería Social[2]). Por esto, la ciberseguridad debe tener en cuenta permanentemente el acceso legítimo a los sistemas críticos de ordenadores que poseen información de todo el sistema y las infraestructuras críticas. Ellas formarán parte de las vulnerabilidades críticas de objeto de estudio por parte del estado mayor del nivel operacional en el planeamiento y ejecución de la campaña (De Vergara y Trama, 2017).

Esta investigación se propone aportar un conocimiento básico inicial para determinar la eficacia de las ciberoperaciones durante el conflicto en el nivel operacional. Para lograr esto, la presente investigación abarcará el desarrollo de los efectos de las ciberoperaciones ofensivas, defensivas, de exploración y de información en las redes que interactúan en el nivel operacional, ejemplificando esto con el conflicto de Estonia en 2007 (De Vergara y Trama, 2017).

Posteriormente, el estudio tratará de abordar en qué momento el centro de gravedad de las ciberoperaciones puede ser considerado el ente primario del cual todo depende en la campaña (PC20-01, 2017). Las Fuerzas Armadas Argentinas, deben comprender que el ciberespacio irrumpió en la forma de vida y los conflictos modernos, hace dos décadas y evoluciona a cada momento. Por tal motivo, prescindir de las ciberoperaciones en la actualidad solo obliga a desarrollar un comportamiento reactivo ante todo lo que plantea el adversario sino, también, estar siempre dentro de su ciclo OODA (observación, orientación, decisión, acción) (Rio, 2013).

Para dar respuesta al interrogante que da motor a la presente investigación, el autor ha establecido como objetivo general el de: identificar cuando el centro de gravedad de las ciberoperaciones puede ser considerado el centro de gravedad de la campaña. Como objetivos particulares, se aspira a enumerar las ciberoperaciones ofensivas y defensivas en las ciberoperaciones, Detallar las ciberoperaciones de información y

[2] Práctica de obtener información confidencial a través de la intrusión de usuarios proyectados (Salis, 2010)

exploración en el Nivel Operacional. Desarrollar los procesos y procedimientos para determinar el centro de gravedad ciberespacial en el nivel operacional.

La hipótesis se funda sobre un abordaje de lo que desarrolla la doctrina en el nivel operacional y los efectos que las ciberoperaciones producen en la actualidad, así como, el desarrollo de los conflictos modernos donde se intenta limitar el enfrentamiento de tropas convencionales. El centro de gravedad de las ciberoperaciones podrá constituirse en el centro de gravedad de la campaña en la fase preparación del nivel operacional.

Este trabajo constituye un aporte a la inclusión para determinar el centro de gravedad en el nivel operacional. Se intentará identificar las posibles operaciones en el ciberespacio del nivel operacional. En ellas, se hará un análisis de las operaciones ofensivas, defensivas, de exploración y de información determinando sus efectos en cada fase de la campaña. Este análisis contribuirá al logro del Estado Final Operacional Deseado y a la protección de aquellos requerimientos críticos propios o a la explotación de las vulnerabilidades críticas del oponente (Kenny, Locatelli, Zarza, 2015).

En el presente trabajo se emplea un proceso metodológico descriptivo desde un enfoque cualitativo sobre conceptos esenciales y sobre la posible aplicación del centro de gravedad de las ciberoperaciones en la campaña del nivel Operacional.

Para la realización del presente trabajo, se recurre primeramente al análisis documental y bibliográfico sobre las publicaciones más recientes presentadas por los países avanzados referentes al objeto de estudio, para luego cotejar con la doctrina propia la mejor articulación dentro del nivel operacional.

También se utilizan, entrevistas en profundidad a profesionales en ejercicio dentro de la estructura de ciberdefensa. Ello sirve a los fines de un mayor acercamiento a la situación que se investiga y permitirá eventualmente capitalizar las lecciones aprendidas con respecto al tema que se analiza. De esta manera y a través de la triangulación intrametodológica, se procura aumentar la validez de la investigación.

En el primer capítulo se realiza una introducción del marco doctrinario y las ciberoperaciones, posteriormente se desarrollan los efectos que persiguen las ciberoperaciones ofensivas y defensivas en el nivel operacional. Para ejemplificar esto, se tiene en cuenta el desarrollo de un conflicto moderno como Estonia 2007.

Posteriormente, en el segundo capítulo se aborda a las ciberoperaciones de exploración e información y a la ingeniería social.

Por otro lado, en el tercer capítulo se analiza el centro de gravedad para llegar a una conclusión de en qué momento el centro de gravedad de las ciberoperaciones puede ser considerado el centro de gravedad dela campaña. Por tal motivo, se intenta demostrar en qué fase de la campaña se planificaría la neutralización del oponente y la protección propia en el nivel operacional.

En función de lo enunciado, se identifica el centro de gravedad de las ciberoperaciones dentro de la campaña, evaluándolo como un elemento del diseño operacional (Kenny, Locatelli, Zarza, 2015).

De esta manera, el centro de gravedad de las ciberoperaciones podrá constituirse en el centro de gravedad de la campaña en la fase preparación del nivel operacional. Visto que, el campo de batalla moderno se libra en la mente de las personas, que el ser humano en la actualidad es ampliamente dependiente de las tecnologías de la información (TIC) no solo para sus relaciones interpersonales, sino también para el desarrollo de diferentes actividades diarias (Llongueras Vicente, 2013). Además de esto, los sistemas de las Fuerzas Armadas mundiales son ampliamente dependientes de las TIC, las cuales por medio de la inteligencia artificial[3], intentan equiparar la Inteligencia humana para el 2050 (Ramió, 2019).

[3] Inteligencia ejecutada por maquinas. Se aplica cuando una máquina imita las funciones cognitivas del ser humano (dentro de las cuales se destacan. Percibir, aprender, razonar y resolver problemas)

## CAPÍTULO I - Las ciberoperaciones ofensivas y defensivas que afectan la campaña

En el presente capítulo se desarrollan las diferentes ciberoperaciones ofensivas y defensivas teniendo en cuenta lo que marca el libro de la Guerra Inexistente la ciberguerra (Llongueras Vicente, 2013), Redes y guerras en red (Arquilla y Ronfeldt, 2003), las Operaciones del ciberespacio de los Estados Unidos de Norteamérica (America, 2018) y, Operaciones Militares Cibernéticas (De Vergara y Trama, 2017), si bien no son prescripciones reglamentarias, estas publicaciones establecen claramente como entienden las ciberoperaciones las diferentes potencias precursoras en este dominio. Por otro lado las Fuerzas Armadas Argentina aún no han dispuesto en sus publicaciones doctrinarias como se subdividen las ciberoperaciones en los distintos niveles de la guerra.

### 1.1 Marco doctrinario y conceptos básicos

La carencia de doctrina en ciberdefensa en el nivel operacional hace necesario que los especialistas en redes informáticas de las diferentes fuerzas establezcan rápidamente conceptos básicos, que permitan trabajar de manera conjunta en este dominio complejo y cambiante. Solo en pocos documentos y directivas del nivel estratégico nacional el poder ejecutivo establece una serie de objetivos y principios rectores (Nacional, Poder Ejecutivo, 2019).

Uno de estos es la Directiva de Política y Defensa Nacional vigente, dónde el poder ejecutivo nombra al ciberespacio como un dominio. También menciona que el desarrollo tecnológico incrementó los riesgos asociados a la militarización de este dominio, la disuasión se ha extendido al espacio cibernético producto de una mayor conectividad, la privacidad y los derechos de la ciudadanía, dando como resultado general la ciberdisuación[4].

Otro documento importante es la directiva de Ciberseguridad de agosto de 2019, donde el estado nacional establece los objetivos y principios rectores que guían este (Nacional, Poder Ejecutivo, 2019)

[4] Según David Simon, es la capacidad en el ciberespacio que tienen las grandes potencias y otros actores para utilizarlas en su competencia geopolítica directa a modo de disuasión para proteger su seguridad nacional. David E. Simon (2017), "Raising the Consequences of Hacking American Companies", Centre for Strategic and International Studies, octubre de 2017.

Por esto, tanto los Estados como los actores no estatales desarrollan medios cibernéticos para explotar las vulnerabilidades inherentes a los sistemas de comando y control, comunicaciones, inteligencia vigilancia y reconocimiento. Además, las redes terroristas explotan el ciberespacio para reclutar miembros, recaudar fondos y difundir propaganda.

También, el despliegue de ciberoperaciones disruptivas está al alcance de naciones menos desarrolladas. El despliegue de esta problemática desde la Defensa Nacional requerirá adoptar medidas desde el punto de vista de la ciberseguridad. Estas medidas facilitarán el resguardo y protección de las infraestructuras críticas del sistema de Defensa Nacional y de aquellas designadas para su preservación.

Para atender la problemática de la ciberseguridad, la Argentina se rige por lo que marca el Comité de Ciberseguridad dentro de la Secretaría de Gobierno de Modernización. Es este Comité del Estado Argentino que tiene la misión de desarrollar la Estrategia Nacional de Ciberseguridad y hacer cumplir los principios y objetivos que marca el Poder Ejecutivo Nacional en el ciberespacio (Nacional, Poder Ejecutivo, 2019).

Por esto, en el presente capítulo se abordan los conceptos referidos a las ciberoperaciones defensivas y ofensivas que afectan la campaña. Para ello, es necesario desarrollar algunos conceptos básicos como ciberdefensa, ciberoperaciones y ciberseguridad. Se considera a la ciberdefensa como un conjunto de acciones ofensivas y defensivas que se ejecutan en el espacio cibernético en preparación o en la planificación y realización de operaciones militares, para asegurar la eficacia de la acción de las fuerzas armadas y el funcionamiento del Ministerio. Ella complementa las medidas de protección de redes, de sistemas y de información con una capacidad de poder operar en el espacio cibernético y una capacidad de gestión de crisis cibernética (De Vergara y Trama, 2017).

Por otro lado, la ciberseguridad son todas aquellas actividades que se ejecutan en el ciberespacio o espacio cibernético contra el uso indebido del mismo, defendiendo sus infraestructuras tecnológicas, los servicios que prestan y la información que manejan (Llongueras Vicente, 2013).

De esta manera se define a las ciberoperaciones, mediante operaciones ejecutadas en el ciberespacio para obtener información, negar, degradar o destruir la información

existente en diferentes dispositivos que operan dentro de una red de computadoras o redes informáticas.

Las ciberoperaciones ofensivas y defensivas operan dentro del ciberespacio, espacio operacional creado tecnológicamente por el hombre donde las organizaciones y personas utilizan las tecnologías de la información y la comunicación (TIC) necesarias para interactuar (Llongueras Vicente, 2013).

### 1.2 Ciberoperaciones ofensivas

Las ciberoperaciones ofensivas se ejecutan en el ciberespacio para comprometer la confidencialidad, la integridad o la disponibilidad de la información del oponente. Estas actividades tienen la finalidad de proyectar el poder en el ciberespacio para obtener los objetivos militares buscando infligir efectos temporales o permanentes a fin de reducir la confianza del adversario en sus redes o capacidades y facilitar las operaciones militares a ejecutarse dentro del teatro de operaciones (De Vergara y Trama, 2017).

De acuerdo cómo las desarrollan países como Estados Unidos, Brasil, Israel y España las ciberoperaciones ofensivas presentan objetivos generales. Estos objetivos sirven para, propagar un virus contaminando el flujo de la información enemiga y los diferentes dispositivos de esa red, controlar los elementos temporales que transitan sobre la internet con la finalidad de alterar la percepción de actores o contener. También se utilizan con la finalidad de interrumpir los sistemas de comando y control del oponente para ejecutar operaciones de información, obtener información, cambiar los datos en las redes (De Vergara y Trama, 2017).

En el uso del componente militar sirven para concentrar los fuegos, las armas y las fuerzas de las propias fuerzas y favorecer la dispersión de las fuerzas enemigas. En cuanto al manejo de información se aplican para diseminar propaganda, transmitir información falsa al enemigo para tergiversar la información real y divulgar información (De Vergara y Trama, 2017).

### 1.3 La cadena de un ciberataque

Según Lockeed Martin Corporation[5], un ciberataque se ejecuta en siete fases. Esto se denomina cadena de un ciberataque donde el ciberatacante intentará crear la

[5] Es una compañía multinacional de origen estadounidense de la industria aeroespacial y militar.

oportunidad para el cumplimiento del efecto deseado. Aquellos que tienen sus redes bien organizadas desde el punto de vista de ciberseguridad, cada una de estas fases es una oportunidad para neutralizar la amenaza. Esta cadena de un ciberataque se puede resumir en las siguientes fases (De Vergara y Trama, 2017):

**Fase reconocimiento:** en esta etapa el ciberatacante busca adquirir la información e inteligencia en el ciberambiente de un blanco del adversario e identificar los objetivos específicos. Estos objetivos manejan datos valiosos en sus redes y presentan alguna vulnerabilidad con respecto a ciberseguridad.

**Fase desarrollo del armamento:** en esta fase los ciberatacantes crean los códigos de computadora (troyano) que generan las condiciones explotando las vulnerabilidades identificadas del sistema a atacar.

**Fase entrega:** en este momento se transmite la carga al sistema de destino usando vectores como: adjuntos de correos electrónicos, sitios web y medios extraíbles (por ejemplo USBs o poniendo un troyano de acceso remoto en un archivo que simula tener información crucial, para incitar al destinatario a ejecutarlo).

**Fase explotación:** una vez que la carga haya sido entregada al sistema de destino, esta fase desencadena la carga, explotando la vulnerabilidad del sistema operativo, si saben que software utiliza el usuario a atacar o servidores se pueden aumentar las posibilidades de esta etapa.

**Fase instalación:** esta fase se utiliza para instalar un acceso remoto o puerta trasera en el sistema de destino que permita al oponente mantener una presencia dentro del sistema infectado.

**Fase mando y control:** en este paso el atacante crea un canal de comunicación para facilitar la transmisión de comandos en forma remota.

**Fase efectos deseados creados:** la última fase permite el atacante lograr sus objetivos de manera remota.

Tabla 1: Medidas de protección para contrarrestar las fases de un ciberataque

| FASE | PROTECCIÓN | OBSERVACIONES |
|---|---|---|
| **Reconocimiento** | Ingeniería social. | El atacante intenta obtener información sobre la organización y sus redes. Busca vulnerabilidades en redes y en IICC. |
| **Desarrollo del armamento** | Parches de seguridad. | El atacante busca explotar las vulnerabilidades encontradas. |
| **Entrega del malware en el sistema** | Sandbox , Ingeniería social. Separar placas de red de la internet e intranet, Anular USB. Evitar drives de MP3; MP4. | El atacante busca alojar el malware en los sistemas. |
| **Explotación del malware insertado** | Sandbox - Limitar uso de Plugs – in. (Java o Flash) | Obtener información. Afectar los sistemas. |
| **Instalación** | Inspecciones SSL. Filtros URL. | El atacante recibe los datos de los ordenadores atacados y puede tomar el control de ellos. |
| **Mando y control** | Monitorear capa 3 y 4 del modelo OSI | Reconocer que el sistema ha sido atacado. |
| **Efectos deseados creaos** | Servidores con información sensible desconectados de internet. | El atacante busca permanecer lo más posible sin ser detectado. |

Fuente: elaboración propia, en base a Operaciones Militares Cibernéticas del General De Vergara y el Contraalmirante Trama.

## 1.4 Efectos de las ciberoperaciones ofensivas

La superpotencia cibernética de los Estados Unidos, a las misiones militares en el ciberespacio la describen por intenciones. Estas ciberoperaciones se ejecutan desarrollando capacidades que permitan generar los efectos en el ciberespacio.

Por esto, un ciberataque está compuesto por las diferentes acciones que crean efectos directos de negación en el ciberespacio, tales como, -degradación, interrupción o destrucción- y la manipulación que conduce a la negación que se manifiesta en los espacios físicos. Las diferentes acciones desarrollan los siguientes efectos **(America, 2018)**:

El efecto de negar se traduce en degradar, interrumpir o destruir el acceso a, operación de, o disponibilidad de un objetivo por un nivel especifico durante un tiempo específico. La negación le impide al adversario el uso de recursos. La descripción de estos efectos es la siguiente:

De acuerdo al párrafo precedente, el primer efecto para negar es degradar, este se utiliza para negar el acceso a una operación de un objetivo en un nivel representado como un porcentaje de capacidad. El nivel de degradación debe ser especificado. Si se requiere un tiempo específico debe ser manifestado oportunamente.

El segundo efecto de negar es interrumpir, este significa negar completamente durante un tiempo el acceso a, o la operación de un objetivo durante un período de tiempo. Normalmente, debe especificarse el tiempo de inicio y de finalización.

La interrupción puede ser considerada un caso especial de degradación donde el nivel de degradación seleccionado es ciento por ciento.

El tercer efecto de negar es destruir, el cual sirve para negar de forma permanente, completa e irreparable. En este efecto las funciones de tiempo y cantidad son maximizadas en el acceso a, o la operación de un objetivo.

El efecto de manipular se utiliza para controlar o cambiar la información del adversario, sistemas de información y/o redes de tal manera que respalden los objetivos del Comandante.

La degradación o destrucción de la capacidad de las redes y los sistemas informáticos enemigos puede realizarse por un tiempo limitado.

La publicación JP 3-12121 Cyberspace Operations establece que "*La ejecución exitosa de operaciones cibernéticas requiere el empleo integrado y sincronizado de las operaciones ofensivas, defensivas y DODIN (operaciones de información en las redes)* (America, 2018) (De Vergara y Trama, 2017)

## 1.5 Ciberoperaciones defensivas

Estas ciberoperaciones son acciones activas y pasivas que se ejecutan en el ciberespacio espacio cibernético para preservar la libertad de acción, para utilizar las capacidades del ciberespacio y proteger datos, redes y capacidades centradas en las redes (America, 2018). Las ciberoperaciones defensivas se enfocan sobre una amenaza específica y vinculan las vulnerabilidades con la intención y capacidad del adversario. De esta manera, se identifican las zonas de riesgo principal donde se deberá focalizar el esfuerzo defensivo (De Vergara y Trama, 2017).

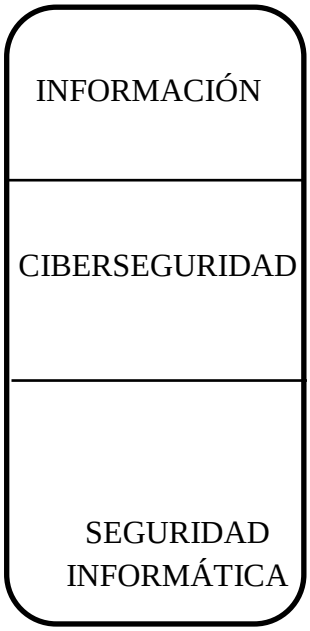
Las acciones activas son aquellas que se ejecutan fuera del entorno propio, para bloquear o detener un ciberataque de manera similar a lo que sería un ataque convencional ejecutado fuera del dispositivo defensivo para defendernos como si fuera un ataque de desarticulación[6]. Sin embargo, acciones pasivas son aquellas que se realizan dentro del propio entorno (De Vergara y Trama, 2017).

## 1.6 Efectos de las ciberoperaciones defensivas

Los efectos en estas ciberoperaciones incluyen proteger, detectar, caracterizar, contrarrestar y mitigar. Tales acciones defensivas son creadas generalmente por el Comandante Conjunto o por la Fuerza Armada específica que posee u opera la red. (America, 2018) (De Vergara y Trama, 2017).

[6] Acción ofensiva planeada por la defensa y ejecutada, normalmente, delante del campo principal de combate cuyo objetivo son fuerzas enemigas que se están organizando o reuniendo para ejecutar un ataque. En su ejecución se debe explotar al máximo la sorpresa. De acuerdo a lo que marca el ROB-00-01 Reglamento para la Conducción de las Fuerzas Terrestres, 2015, Cap IV pág 8.

Tabla 2. Relaciones entre las ciberoperaciones y el ciberespacio.

| **Ciberoperaciones** | **EFECTOS** | **CIBERESPACIO** |
|---|---|---|
| Ofensivas | Negar, degradar, interrumpir, destruir, manipular. |  |
| Defensivas (Activas / Pasivas) | Proteger, detectar, caracterizar, contrarrestar y mitigar. | |
| Exploración | Detectar y neutralizar. | |
| Información | Manipular, neutralizar, desgastar. | |



Fuente: elaboración propia, del dominio ciberespacio y su interacción permanente con las ciberoperaciones en base al JP 3-12 Cyberspace Operations, junio 2018, pág II-3, Primer Seminario de Ciberdefensa y Ciberseguridad en la Argentina y Curso de Ciberdefensa y Ciberseguridad dictados en la Escuela Superior de Guerra Conjunta.

## CAPÍTULO II - Ciberoperaciones de exploración e información.

El propósito de este capítulo es determinar las ciberoperaciones de exploración e información y sus efectos. Para alcanzar este objetivo se completa el análisis de las diferentes ciberoperaciones desarrolladas en el capítulo, con conceptos de ingeniería social. También se propone la incorporación de la matriz de Tobias Fekin modificada por el Dr Roberto Uzal en el planeamiento del nivel operacional. Estos conceptos se desarrollan de acuerdo a lo que marca el manual de Operaciones Cibernéticas de (De Vergara y Trama, 2017), la publicación de Operaciones del Ciberespacio de las Fuerzas Armadas de Estados Unidos (America, 2018) y, la Ciberguerra, la guerra Inexistente de Adrianna Llongueras Vicente (Llongueras Vicente, 2013).

### 2.1 Ciberoperaciones de exploración y efectos:

Son aquellas actividades que se ejecutan en las redes para obtener datos, siendo el fin último de estas detectar vulnerabilidades, debilidades y amenazas (America, 2018).

Las potencias desarrolladas en el ciberespacio como Estados Unidos y Rusia dividen la exploración, en dos fases. En la primera se concentran en la recopilación de información, que atacan principalmente el software, hardware, el personal que opera las diferentes redes o sistemas y las políticas de seguridad informática operacional, como la conformación de sus redes desde el punto de vista de ciberseguridad. La segunda fase o ciberoperación se concentra en generar las condiciones para vulnerar un sistema más sofisticado, del cual, ya se posee la información básica pero se precisa de datos específicos, avanzados y actualizados para sostener un efecto por un tiempo determinado (De Vergara y Trama, 2017), (America, 2018).

En el nivel operacional lo más correcto en las ciberoperaciones de exploración es hablar de acciones dirigidas contra los sistemas de tecnologías que protegen las infraestructuras críticas o el centro de gravedad del oponente. Estas ciberoperaciones serán ejecutadas para obtener información relevante que permitan producir un nuevo conocimiento de la situación y de esta manera detectar las vulnerabilidades en el oponente. Además dirigir sobre estas vulnerabilidades ciberataques que permitan, interrumpir, negar, degradar, corromper o destruir, la información almacenada en redes de computadoras, dispositivos o comunicaciones del oponente (De Vergara y Trama, 2017).

A pesar de esto, esta información también sirve para proteger nuestro centro de gravedad cibernético contra cualquier ciberataque y permitir organizar un dispositivo que sea lo suficientemente resiliente para poder contrarrestar estos ciberataques en contra de los dispositivos de origen. Este último permite aumentar la eficiencia de las redes, los diferentes dispositivos que interactúan en ellas y sistemas de armas mejorando de manera proactiva su ciberseguridad ante una posible situación de conflicto (Corletti Estrada, 2017), (De Vergara y Trama, 2017).

Otra herramienta que garantiza el correcto desempeño de una red dentro del hacking ético[7] es un penetration test, la cual ataca software, sistemas de computadoras y puertos para ejecutar un informe por períodos cortos. En períodos largos se utilizan los Red Teams en ciberoperaciones ofensivas, Blue Teams en ciberoperaciones defensivas o, Purple Teams en metodología integradora del equipo Rojo y Azul. Este último sería al más apropiado para chequear los efectos y detectar vulnerabilidades en el nivel operacional (Miessler, 2019).

Finalmente, teniendo en cuenta lo que el nivel estratégico nacional desarrolla en la última Directiva de Política y Defensa Nacional con respecto a la vigilancia y control del ciberespacio. El Nivel Operacional debe poseer las capacidades necesarias que le permita en las ciberoperaciones en desarrollo o ante la conformación de un Teatro de Operaciones neutralizar cualquier tipo de amenaza. Para lograr eso, debe conducir las capacidades de vigilancia y control del ciberespacio a fin de anticipar y prevenir ciberataques y ciberexplotación en las redes informáticas que afecten cualquier Sistema de Defensa dentro del TO (Nacional, 2018).

También conduce ciberoperaciones para proteger la infraestructura crítica del país o la información que posibilite el acceso a ellas. Esta misión la desarrollara bajo la supervisión y el control del Comando Conjunto de Ciberdefensa y las diferentes agencias del estado. Los efectos que excedan al Comandante del Teatro de Operaciones se requerirán a la estrategia Nacional (Nacional, 2018).

### 2.2 Ciberoperaciones de información y efectos:

Las ciberoperaciones de información buscan alterar el proceso de toma de decisiones en el oponente utilizando el ciberespacio. Un error frecuente es tratar de diferenciar

[7] Hacking ético. Según el manual de Ethical Hacking en su glosario dice que, es el acto de una persona al usar sus conocimientos de informática y seguridad para realizar pruebas en redes y encontrar vulnerabilidades, con el objeto de reportarlas y que se tomen medidas sin producir daño.

aquellas ciberoperaciones que se desarrollan en el ciberespacio, tipificándolas como operaciones de información (De Vergara y Trama, 2017).

A pesar de que el control del ciberespacio otorga poder, también genera vulnerabilidades como puede ser la transmisión en tiempo real de imágenes o hechos por parte de los habitantes que condicionan el proceso de toma de decisiones de las Fuerzas Armadas dentro del Teatro de Operaciones. Esto facilita la divulgación de información secreta otorgándole ventajas al oponente. La saturación de mensajes a través de las redes sociales dificulta el control y hace mucho más compleja la información y desinformación (De Vergara y Trama, 2017).

Por esto, las ciberoperaciones de información persiguen efectos que solo ellas pueden ejecutar y, en todo momento buscaran otorgar libertad de acción para la ejecución de la maniobra y la conquista del objetivo operacional que coadyuven con el logro del efecto operacional deseado. Por tal razón, es pertinente vincularlas con las ciberoperaciones ofensivas y defensivas que busquen proteger el proceso de toma de decisiones propio e intenten alterar el del adversario (De Vergara y Trama, 2017). El desarrollo de estas capacidades lograra introducir al oponente en el ciclo OODA (observación, orientación, decisión y acción) propio, lo cual contribuirá a la desarticulación del adversario (Rio, 2013).

El desarrollo de estas ciberoperaciones cobra gran importancia a lo largo de toda la campaña. Sin embargo el momento más sensible para desarrollarlas es durante la fase preparación donde se buscara inducir al enemigo erróneamente, buscando alterar su percepción sobre el conflicto y demás componentes que participan en el TO (PC20-01, 2017). El principal efecto a perseguir en esta fase de la campaña será manipular a quien debe tomar la decisión final para evitar el conflicto convencional y, como decía Sun Tzu, vencer al oponente sin entrar en combate abierto.

Por lo descripto anteriormente, las ciberoperaciones de información buscan explotar el uso de las capacidades del ciberespacio. Por esto, las ciberoperaciones ejecutadas en las redes informáticas tienen por finalidad modificar los datos o algoritmos de una red o sistema para que se produzcan resultados contrarios a los que se esperaban, estas conforman parte de las ciberoperaciones a ejecutar para generar las condiciones dentro del TO (De Vergara y Trama, 2017).

Sin embargo el elemento determinante en este sistema hombre máquina, sigue siendo el factor humano, el cual se reconoce en ciberdefensa como ingeniería social.

### 2.3 Ingeniería Social:

El eslabón más débil de todo sistema donde se maneja información es el hombre. La ingeniería social es el arte de engañar a las personas para convencerlas de que ejecuten las acciones o actos que el atacante necesite para lograr su cometido. Para esto se utiliza técnicas psicológicas y habilidades sociales de manera consciente y premeditada (Salis, 2010).

Un ingeniero social, usa por lo general internet o el teléfono para engañar a otros usuarios de relevancia. Una forma de acceder es fingir ser el proveedor de algún servicio, un compañero de trabajo o un cliente, donde a través de mensajes enviados por internet de aparente procedencia legal, se obtiene información confidencial (Salis, 2010).

De esta manera los ingenieros sociales aprovechan la tendencia general de la gente a confiar y reaccionar en forma predecible en ciertas circunstancias ante los datos que recibe por internet o vía telefónica obteniendo información sin la necesidad de vulnerar un algoritmo u otro sistema (Salis, 2010), (De Vergara y Trama, 2017).

Un icono de esto para el gobierno de los Estados unidos fue Edward Snowden quien después de trabajar como antiguo empleado de la CIA y la NSA traicionó a su país de origen. Actualmente, este hacker vive en Rusia exiliado y vende sus servicios a otras potencias o diferentes organizaciones cibernéticas. Este caso es de gran relevancia porque, se trata de un hacker con capacidades ilimitadas cuando es respaldado por potencias opositoras o diferentes organizaciones (Snowden, 2019).

Por esto, las empresas que se dedican en la actualidad al cibercrímen[8] o los estados que intentan manipular permanentemente la percepción de las personas para obtener un beneficio trabajan sobre la ciberconfianza[9]. Por esto, los estados, organismos de

[8] Acción antijurídica que se realiza en el entorno digital, espacio digital o Internet.
[9] Según el glosario de ciberseguridad. Esperanza firme que una persona tiene en que algo suceda, sea o funcione de una forma determinada en el espacio digital o ciberespacio.

ciberdefensa y ciberseguridad para frenar esta ciberguerra[10] permanente desarrollan la ciberdisuación[11] (De Vergara y Trama, 2017).

### 2.4 Lineamientos metodológicos para elaborar una respuesta adecuada ante un ciberataque perpetrado o apoyado por otro Estado Nación con el empleo del poder militar

Estos lineamientos tienen el objeto de establecer posibles respuestas luego de haber desarrollado todas las ciberoperaciones y sus efectos. Las respuestas a un ciberataque pueden ejecutarse en forma complementaria de las respuestas de las relaciones internacionales, económicas o del empleo del poder convencional militar. Estas se ejecutarán con dificultad si el gobierno no incorporó previamente capacidades en este dominio (Uzal, 2015).

Por esto, el reconocimiento de una ciber respuesta a un ciberataque en forma pública puede ser leído como incorrecto políticamente. Esto podría causar la pérdida de legitimidad internacional contra otros objetivos en un futuro. Para evitarlo, en general se utilizan respuestas *proxies* - servidores de comando y control desplegados.

Los tiempos de respuesta para accionar frente a un ciberataque del nivel operacional y estratégico son escasos, los estados mayores deben elaborar un marco general que catalogue respuestas alternativas tipo ante la ocurrencia de un ciberincidente[12] disruptivo o destructivo con el empleo del poder militar.

Si bien no hay conflicto igual a otro, este marco general le proveerá a las autoridades civiles y militares diferentes opciones de respuestas generales. Un esquema que contribuye al proceso de toma de decisiones se desarrolla en la matriz de Tobias Feakin modificada por el Doctor Uzal. Esta matriz debe ser perfeccionada por los integrantes del elemento de defensa cibernética a nivel operacional y estratégico (Uzal, 2015).

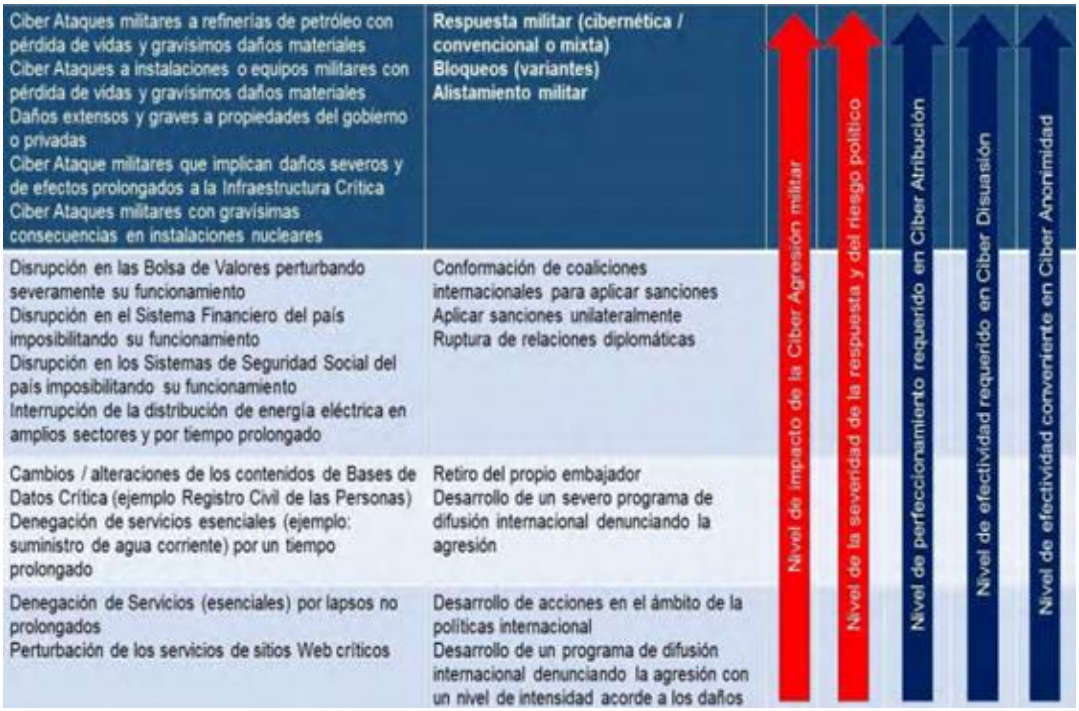
---

[10] Según el glosario de ciberseguridad. Es un área que tiene como objetivo encontrar las vulnerabilidades técnicas de los sistemas o redes informáticas del enemigo para penetrarlas y atacarlas a fin de extraer datos e información sensible.

[11] Para el Dr Roberto Uzal es lograr que los estados naciones agresores, reales y potenciales, perciban claramente que los costos esperados, económicos, políticos, militares, geopolíticos y de imagen asociados a una Ciber Agresión a la Infraestructura Crítica Nacional de otro estado nación, superan ampliamente a los resultados esperados de dicha hipotética Ciber Agresión. En síntesis: Que no atacar sea percibido claramente como un mejor negocio que atacar.

[12] Según el glosario de ciberseguridad. es un hecho que se produce en el transcurso de un asunto en el ciberespacio y que repercute en él alterándolo o interrumpiéndolo.

Tabla 3: Matriz de Tobias Fekin modificada por el Doctor Roberto Uzal




Fuente: elaboración del Dr Uzal, matriz de Tobias Feakin modificada por el Doctor Uzal. La cual contribuye al proceso de Toma de Decisiones en la planificación del Nivel Operacional (Uzal, 2015).

Esta herramienta de ciberrespuestas ante un ciberataque detalla en su primera columna ejemplos de diferentes ciberagresiones. Posteriormente, en la segunda columna se desarrollan distintos tipos de respuestas a las ciberagresiones expuestas. La flecha de la tercera columna marca el crecimiento de los daños causados por potenciales ciberagresiones militares, por otro lado la cuarta columna indica el nivel creciente de severidad, la potencial respuesta a una ciberagresión militar. La quinta columna indica, la importancia que la Argentina incorpore capacidades para resolver las variantes del problema de atribución, aspectos que están completamente relacionados con la ciberdisuación y la ciberanonimidad. Seguidamente, en la sexta columna esta flecha indica el nivel de efectividad en ciberdisuación que debería contar para cada caso para no ser considerado un blanco fácil. Finalmente, la séptima columna indica el nivel de ciberanonimidad requerido para cada caso (Uzal, 2015).

La Matriz de Tobias Feakin modificada facilita la identificación de los componentes a las respuestas de ciber incidentes generales. El conocimiento de estos componentes otorga al conductor político y militar variables ante un ciberataque (Uzal, 2015).

## CAPÍTULO III - Procesos y procedimientos para determinar el centro de gravedad ciberespacial en el nivel operacional

El propósito de este capítulo es determinar en qué fase de la campaña el CGD de las ciberoperaciones puede ser considerada el centro de gravedad de toda la operación en el Teatro de operaciones. Para conseguir este objetivo se realiza un análisis general de los factores críticos que afectan al nivel operacional, y abordar finalmente a la identificación del CDG ciberespacial. Estos conceptos se desarrollan de acuerdo a lo que marca la doctrina de Estados Unidos y del Brasil esencialmente, además se describe el CDG utilizando la doctrina conjunta (PC20-01, 2017) y, Arte y diseño operacional (Kenny, Locatelli, Zarza, 2015). La doctrina y las conclusiones extraídas de diferentes fuentes bibliográficas sirven para dar mayor claridad a la determinación del CGV, en los conflictos actuales.

### 3.1 Centro de Gravedad Cibernético

La respuesta cinética[13] de Israel a un supuesto ciberataque palestino en el mes de mayo de 2019 deja claro que las potencias cibernéticas consideran a las ciberarmas[14] como a otros sistemas de armas de la guerra convencional con la capacidad de producir daños superiores a cualquiera de ellos. Esto se relaciona directamente con la determinación del CDG desde que quedo confirmado que las ciberarmas tienen efectos físicos y cinéticos (De Vergara y Trama, 2017).

La determinación del Centro de gravedad[15] propio y del oponente es una de las actividades más importantes de todo estado mayor del nivel operacional (PC20-01, 2017). Empero, un aspecto importante a tener en cuenta en el campo de batalla actual es que el combate, se libra en forma permanente en la mente de las personas debido a la dependencia cada vez mayor de las nuevas tecnologías. Por tal razón, solo aquel que tiene las capacidades para controlar parcialmente el ciberespacio, posee un sistema ciber resiliente[16] en este dominio (Corletti Estrada, 2017).

[13] Acto de atacar desde el espacio una parte de la superficie terrestre con un proyectil donde la fuerza destructiva proviene de la energía cinética liberada durante impacto del proyectil.
[14] Según Kaspersky, compañía Rusa dedicada a la seguridad informática. Una ciberarma es un tipo de código malicioso, script, llámese como sea, destinado normalmente para atacar y defender en el espacio cibernético. Ejemplo de esto es Stuxnet o Flame.
[15] Según Eikmeier el CDG es el ente primario que tiene la capacidad inherente de alcanzar el objetivo. El Manual de Arte y Diseño Operacional lo tipifica como un elemento innovador del diseño operacional.
[16] Según el Doctor Roberto Uzal es la capacidad de volver un sistema a su estado inicial.

Por tal razón, la ciberresiliencia se logra cuando la ciberseguridad se desarrolla de manera eficiente y es capaz de resistir un ciberataque, detectarlo, neutralizarlo y volver el sistema a su estado inicial. A pesar de que la ciberseguridad, se la asocie con las ciberoperaciones defensivas y, que en el nivel operacional en los otros dominios el esfuerzo principal se encuentre en la defensa, en las ciberespacio no sucede eso. En el ciberespacio la libertad de acción la otorgan las ciberoperaciones ofensivas. Estas son las únicas que tienen la capacidad de garantizar el funcionamiento del sistema de comando y control, las diferentes redes, la información y las infraestructuras críticas (Estrada, Ciberseguridad, Una Estrategia Informático/Militar., 2017), (De Vergara y Trama, 2017).

La legitimidad[17] en este dominio hace que a las ciberoperaciones defensivas se las relacione con el esfuerzo principal. Otro aspecto a destacar es el marco legal vigente actual que, al ser difuso cuando se menciona un ciberataque y el despliegue de medios que necesita para sostener un efecto en el nivel operacional es muy superior. Esto hace que para el desarrollo de un sistema ciberresiliente debe ser tratado de manera interagencial con todos los organismos del estado y privados (De Vergara y Trama, 2017).

Según Alejandro Corlletti Estrada la mejor forma de organizar el dispositivo de nuestro sistema cibernético es como una acción retardante, ya que esta otorga un mayor dinamismo para la ejecución de las ciberoperaciones (Estrada, 2011).

La determinación del tipo de ciberoperación a ejecutar es trascendental en el momento de analizar el CDG ciberespacial propio y del oponente, ya que esta me permite durante la planificación identificar las capacidades críticas (CC)[18], los requerimientos críticos (RC)[19] y las vulnerabilidades críticas (VC)[20] (Kenny, Locatelli, Zarza, 2015).

[17] Consenso o acuerdo entre los miembros de una comunidad, el cual es referido a valores culturales, normas y niveles más profundos y detallados.

[18] Según Strange, son las habilidades primarias que ameritan que un Centro de Gravedad sea identificado como tal en el contexto de un escenario, situación o misión dados. (Kenny, Locatelli, Zarza, 2015, pág. 66)

[19] Según Strange, son condiciones, recursos y medios que son esenciales y que hacen que una capacidad crítica sea totalmente operativa. (Kenny, Locatelli, Zarza, 2015, pág. 67)

[20] Según Strange, son requerimientos críticos o componentes de ellos que son deficientes o vulnerables a la neutralización, interdicción o ataque, que permiten alcanzar resultados decisivos. (Kenny, Locatelli, Zarza, 2015, pág. 68)

La dependencia de nuestros sistemas de armas de las TIC conforma una vulnerabilidad crítica, por tal motivo los Comandantes en el nivel operacional centran sus esfuerzos en la protección de estos sistemas para evitar que se generen debilidades (De Vergara y Trama, 2017).

El Comandante del TO debe analizar sus capacidades cibernéticas, las del oponente y aquellas organizaciones de otro tipo que dispongan de estas capacidades para interferir o neutralizar su sistema de comando y control. Además solicita el apoyo de las capacidades cibernéticas de la estrategia nacional cuando se trate de proteger el CDG cibernético propio o neutralizar el del oponente (De Vergara y Trama, 2017).

### 3.2 Análisis de los factores críticos del Centro de Gravedad cibernético

Los factores críticos (capacidades críticas, requerimientos críticos y vulnerabilidades críticas), son los elementos que todo Comandante y su Estado Mayor en el Nivel Operacional debe analizar para proteger o neutralizar el CDG (Kenny, Locatelli, Zarza, 2015) . La eficiencia se logra si el elemento cibernético posee el poder de combate y alcance operacional necesario para proteger y afectar los factores críticos propios y del oponente (Kenny, Locatelli, Zarza, 2015).

La doctrina argentina establece que un CDG genera una o varias CC, estas funcionan de manera sistémica otorgando poder, libertad de acción y equilibrio (PC20-01, 2017).

De estas capacidades se desprenden los requerimientos críticos que hacen que estos se comporten como un sistema. Sin embargo lo más importante a detectar por el Departamento de Comunicaciones y Ciberdefensa en el Estado Mayor del nivel Operacional son las vulnerabilidades críticas. Estas debilidades surgen después de un intenso análisis del CDG ciberespacial propio y del oponente, las mismas son consideradas puntos decisivos[21] cuando la fuerza puede operar sobre ellas. Además, estas VC ofrecen oportunidad para minimizar costo y mantener la iniciativa (Kenny, Locatelli, Zarza, 2015).

Un aspecto importante a diferencia de las fuerzas militares que operan en los tres dominios tradicionales (terrestre, aéreo y naval), es que el elemento o sistema que

[21] Según Alejandro Kenny, Omar Locatelli y Leonardo Zarza, son un conjunto de condiciones, vinculadas a ubicaciones geográficas, sucesos específicos claves, sistemas de capacidades, funciones críticas o entorno de la información, que cuando se alcanzan permiten al Comandante del TO, influir de sobremanera en el resultado de la maniobra operacional o de la campaña (Kenny, Locatelli, Zarza, 2015, pág. 78)

opera en el ciberespacio puede alcanzar factores críticos que en la antigüedad eran muy difícil, como la empatía de una determinada población, la cual puede condicionar la libertad de acción de un Comandante en el Teatro de Operaciones (TO). Según Milan Vego, en la era de la información surge un nuevo concepto, el "*punto decisivo cibernético"* (Vego, 2007), debido a la dependencia de las comunicaciones e informática de los sistemas de armas que operan en el TO. Esto facilita que el ponente interrumpa nuestro sistema de comando y control a grandes distancias que exceden al TO. (De Vergara y Trama, 2017)

Por esto, es importante que el Comandante del nivel operacional incluya el ciberespacio como dominio durante la planificación, esto le permitiría reforzar el sistema defensivo y establecer alternativas ante posibles amenazas (De Vergara y Trama, 2017).

Por otro lado, según lo que marca Williams Brett, para estar en condiciones de ejercer el comando y control el Comandante del TO debe conocer la arquitectura del sistema cibernético. Este sistema lo descompone en cinco componentes, la infraestructura de comunicaciones que incluye redes alámbricas en inalámbricas, redes que organizan y distribuyen información, capas de protección, conocimiento de herramientas para desplegar información que faciliten el proceso de toma de decisiones y sensores que entregan inteligencia, vigilancia y reconocimiento (Brett, 2011).

El conocimiento de esta arquitectura del sistema cibernético básica, permite estar en condiciones de analizar las capacidades críticas del CGV cibernético. Estas son las habilidades primarias que identifican al CDG en el contexto de un escenario, situación o misión dados (Kenny, Locatelli, Zarza, 2015, pág. 66).

### 3.3 Método para determinar el Centro de Gravedad cibernético

Según Eikmeier el CDG es, *"el ente primario que tiene la capacidad de alcanzar el objetivo"* y teniendo en cuenta que una de las tareas más importantes del diseño operacional que enfrenta un Estado Mayor es la identificación del CDG. El análisis sistémico aporta una herramienta analítica que permite identificar fortalezas y debilidades propias y del oponente (Kenny, Locatelli, Zarza, 2015).

El método más apropiado que presenta ventajas para determinar el CDG y analizar en profundidad los factores críticos es el de la teoría de los sistemas *"fines, modos y*

*medios"*[22]. Este método se desarrolla en ocho pasos cuatro para determinar el CDG ciberespacial y cuatro pasos para determinar los requerimientos críticos y vulnerabilidades críticas que se deben afectar o proteger del CDG ciberespacial (Kenny, Locatelli, Zarza, 2015).

Tabla 4. Método de determinación del Centro de Gravedad Ciberespacial. "FINES, MODOS Y MEDIOS"

| PASOS | TAREA |
|---|---|
| PASO 1 | Identifique los fines u objetivos del elemento bajo análisis |
| PASO 2 | Identifique los modos o acciones cibernéticas posibles que le permitan a ese actor alcanzar ese fin y los modos del propio sistema. |
| PASO 3 | Enumere los medios de la organización disponibles o necesarios de ciberdefensa para realizar el modo/CC. |
| PASO 4 | Del listado de medios elija el ente cibernético que tiene la CC de alcanzar el Objetivo |
| PASO 5 | De los ítems remanentes del listado de medios. Elija aquellos críticos para ejecutar la CC. Estos son los RC del CDG ciberespacial. |
| PASO 6 | Identifique los RC vulnerables a las acciones del oponente. |
| PASO 7 | Identifique en los RC del oponente las VC. |
| PASO 8 | Relacione las VC con los puntos decisivos. |

Fuente: elaboración propia, para determinar el CDG ciberespacial durante el planeamiento del NO en base al manual de Arte y diseño Operacional, pág 71, de Kenny, Locatelli y Zarza y lo desarrollado en el Ejercicio Alianza.

El campo de batalla actual se está librando en la mente de las personas, teniendo en cuenta que las operaciones en el ciberespacio se basan en efectos y uno de ellos es manipular la realidad. Es pertinente analizar los elementos en capacidad de producir estos efectos, ya que los mismos pueden tener consecuencias superiores a los de cualquier arma convencional (De Vergara y Trama, 2017).

Por esto, en el análisis de los factores críticos lo más importante es determinar los RC el cual es un elemento vital dentro del sistema, Estos se deberán atacar para producir la vulnerabilidad y como consecuencia, afectar o neutralizar el CDG del

[22] Según Eikmeier Dale, este método brinda mayor certidumbre y menos discusión al responder a tres preguntas simples: ¿cuál es el objetivo?, ¿cómo lo puedo alcanzar? Y ¿qué recursos se requieren?. Eikmeier Dale. "Redefining the Center of Gravity". Op.cit. Pag158.

oponente. Esta vulnerabilidad constituye el foco hacia donde se materializa la maniobra (PC20-01, 2017). Según William Brett, un análisis de la situación exhaustivo me permite identificar cuando hay varios sistemas involucrados, con sus diferentes vulnerabilidades. La vinculación de estas vulnerabilidades y la intención y capacidad del adversario dan como resultado la zona de riesgo donde se debe incrementar el esfuerzo de la defensa (Brett, 2011).

### 3.4 Relación de la campaña con el CDG cibernético

Por otro lado, según nuestra doctrina conjunta dice que la campaña es un conjunto de operaciones militares que se ejecutan en un tiempo y espacio dados (PC20-01, 2017). También está, se desarrolla en tres fases, preparación, ejecución y estabilización donde el estado mayor del nivel operacional planifica el diseño operacional de la campaña[23]. La fase preparación es la que se ejecuta para generar las condiciones del desarrollo de la maniobra operacional[24], en esta fase cada línea de operación tiene un rol trascendental para el desarrollo de las operaciones militares, porque conectan a la fuerza propia con los objetivos (PC20-01, 2017).

Por lo expuesto anteriormente, el centro de gravedad ciberespacial puede coincidir con el centro de gravedad de la campaña durante la fase preparación, ya que es el momento más propicio para afectar el proceso de toma de decisiones e influir en la percepción emocional de diferentes actores involucrados que modifiquen la situación. Esta afirmación se fundamenta en que el campo de batalla moderno se está librando permanentemente en la mente de las personas, donde existen numerosas herramientas informáticas que permiten establecer un perfil de cada ciudadano y manipular su percepción emocional[25] (De Vergara y Trama, 2017).

[23] Según el manual de Arte y diseño operacional es la concepción y construcción de un marco que sustenta la campaña y su ejecución (Kenny, Locatelli, Zarza, 2015, pág. 47)

[24] Según el manual de Arte y diseño operacional es la combinación de esfuerzos operacionales, a ser llevados a cabo mediante el mejor empleo de los recursos y fuerzas disponibles, en un tiempo y espacio dados para alcanzar un Objetivo Operacional (Kenny, Locatelli, Zarza, 2015, pág. 55)

[25] Según Daniel López Rosetti en su libro Equilibrio Kant decía, lo que cada ser percibe se encuentra modificado por nuestra subjetividad. Por tal motivo lo que uno concibe como realidad puede resultar parcialmente diferente de los demás, porque la noción de realidad se modifica con nuestros pensamientos y sentimientos (López Rosetti, 2019, págs. 123-124).

### 3.5 Ejemplo de análisis de factores cibernéticos

El ejemplo de este análisis se desarrolla en la Tabla 5. En este, se analiza una situación simulada reducida dónde, el sistema e infraestructura de información militar de Israel, según analistas Iraníes es un CDG porque tiene la capacidad de integrar sistemas de información militar y civil aprovechando sus capacidades de acceso global para actividades de combate (De Vergara y Trama, 2017).

Tabla 5. Ejemplo reducido de análisis de Factores cibernéticos

| **CDG CIBERESPACIAL** | **CC** |
|---|---|
| Sistema e infraestructura de comunicaciones de Israel | Implementar ciberataques contra los sistemas e infraestructura de sistemas de información por medios manuales propios y utilizando a Rusia como proxy |
| | Infectar los sistemas de información militar del enemigo con virus informáticos, gusanos o malware para robar o reunir información infiltración en los sistemas o spear fishing – Stuxnet/Flame-. |
| | Implementar ataques DDOS |
| VC | RC |
| Falta de especialistas cibernéticos talentosos y especialistas en los ámbitos de planificación de las organizaciones militares. | Formar un equipo de redes sociales que trabaje permanentemente |
| Uso limitado de actividades de ciber información. | Un gran número de computadoras zombies y botnets |

Fuente: elaboración propia modificada del ejemplo de Análisis presentado por el Grl Evergisto De Vergara y el Contraalmirante Adolfo Trama en el Manual de Operaciones Militares Cibernéticas de Karaman y otros.

# CONCLUSIONES

## Conclusiones al primer objetivo:

Para dar respuesta al primer capítulo, el objetivo específico persigue: Enumerar las operaciones ofensivas y defensivas en ciberoperaciones que afecten la campaña.

La descripción de los dos tipos de ciberoperaciones con sus efectos permite tener un análisis general de las principales causas y consecuencias de las operaciones en el ciberespacio. Esto coadyuva a entender que, la obtención de la superioridad en el ciberespacio es un prerrequisito para la efectividad de las operaciones militares en todos los dominios. La pérdida del control en este dominio se traduce en la carencia de comunicaciones fiables, de precisión, lo cual dificultará el comando y control del Comandante en el Teatro de Operaciones.

Por lo anteriormente mencionado, el nivel operacional junto al nivel estratégico deben trabajar para evitar que la aparición de cualquier ciberamenaza ponga en peligro las diferentes infraestructuras críticas como los objetivos de valor estratégicos de la nación argentina.

Para lograr esto, es necesario desarrollar capacidades de respuesta cibernética que permitan responder a un posible ciberataque y estar preparados para entrar en acción de forma proactiva. Esto permitirá ser efectivos en cuanto a la ciberresiliencia en las estrategias de ciberseguridad y estar en capacidad de recobrar la iniciativa.

La alta dependencia de los medios militares a las TIC los expone como un objetivo rentable a ciberataques, este aspecto se puede comprobar en la actualidad ya que las principales potencias, organizaciones supraestatales y ejércitos están llevando el conflicto al espacio cibernético. Por esto, es fundamental abordar la ciberdefensa de manera pasiva y activa, protegiendo las infraestructuras críticas por parte de las fuerzas armadas como lo marca la Directiva de Política y Defensa Nacional vigente.

Por tal motivo, afirmando lo que el General De Vergara y el Contraalmirante Trama sostienen en el Manual de Operaciones Cibernéticas, las ciberoperaciones de defensa pasiva serán conducidas por el Comandante que tenga autoridad sobre el ciberespacio a proteger. Mientras que, las ciberoperaciones de defensa activa requerirán al nivel estratégico la autoridad delegada, la cual estará condicionada por los efectos que tendrán impacto negativo sobre los diferentes nodos agresores. La

toma de decisiones oportunas sobre las ciberoperaciones defensivas a ejecutar otorgará libertad de acción al Comandante del nivel Operacional.

**Conclusiones al segundo objetivo:**

El segundo capítulo de este trabajo busca responder el objetivo de: Detallar las ciberoperaciones de información y exploración en el Nivel Operacional.

En el nivel operacional, según mi opinión lo más correcto en las ciberoperaciones de exploración es hablar de acciones dirigidas contra los sistemas de tecnologías que protegen las infraestructuras críticas. Sin embargo, el mundo cibernético actual pone en duda si lo más importante es la infraestructura crítica o la información que manejan las redes de esa infraestructura crítica. Por esto, es importante entender que el eslabón más débil de todo sistema donde se maneja información es el hombre, más del setenta por ciento de las vulnerabilidades surgen por una falla humana. La ingeniería utiliza técnicas psicológicas y habilidades sociales de manera consciente y premeditada, por tal motivo se debe trabajar permanentemente sobre políticas de seguridad para mitigar la ciberconfianza que el ingeniero social busca crear en su entorno.

No obstante, las ciberoperaciones de información buscan otorgar libertad de acción y generar las condiciones para el logro del efecto operacional deseado.

Finalmente, un ejemplo claro de un ciberataque y las falencias de un estado en los aspectos desarrollados en este objetivo fue el conflicto de Estonia del 2007. En dicho conflicto, uno de los países más desarrollados tecnológicamente como Estonia sufrió un ataque de denegación de servicios masivo, el cual no presentó víctimas pero paralizó las actividades financieras y gubernamentales durante semanas.

**Conclusiones al tercer objetivo:**

El contenido del tercer capítulo sigue la pregunta de: Desarrollar los procesos y procedimientos para determinar el centro de gravedad ciberespacial en el nivel operacional.

Para responder a este interrogante se explica un proceso reducido para determinar el CDG de las ciberoperaciones como un elemento innovador del diseño operacional, relacionándolo con la campaña del nivel operacional. Un aspecto fundamental a tener en cuenta es, que el campo de combate moderno se está librando permanentemente en la mente de las personas, diferentes organizaciones privadas y estatales manipulan

la percepción emocional de las personas. También los elementos cibernéticos en la actualidad producen respuestas más destructivas que cualquier arma convencional.
Por otro lado, el factor más influyente sobre el nivel operacional es la alta dependencia de los sistemas de armas con respecto a las nuevas tecnologías. Estos factores hacen que el CDG de las ciberoperaciones tenga un papel protagónico en el campo de batalla actual y futuro.

**Conclusiones a la pregunta de Investigación:**

El interrogante que da origen a esta investigación es, ¿Cuándo el centro de gravedad de las ciberoperaciones puede ser considerado el centro de gravedad de la campaña?

Se puede afirmar que, hace más de dos décadas, el ciberespacio se ha convertido en el centro de gravedad del poder nacional, financiero, diplomático y militar de cualquier estado nación que le importe el bienestar y la privacidad de sus ciudadanos.

El campo de batalla actual se está librando en la mente de las personas, teniendo en cuenta que las operaciones en el ciberespacio se basan en efectos y uno de ellos es manipular la realidad. Es pertinente llegar a la conclusión que el momento más propicio para que el CDG de las ciberoperaciones coincida con el de la campaña es durante la fase preparación. En esta afirmación se tiene en cuenta que no hay un conflicto igual al otro. Sin embargo, los conflictos actuales tienen algo en común que es la influencia sobre la percepción emocional de las personas debido a la alta dependencia de las tecnologías de la información en la vida humana.

Por otro lado el dominio del ciberespacio debe estar en todo diseño operacional y solo puede ser tratado por aquellos soldados que tienen el conocimiento y, la experiencia para planificar, organizar, controlar, coordinar y dirigir esta dimensión.

La naturaleza de la guerra subjetiva de Clausewitz cambió, por lo cual solo los cibersoldados que siempre menciona el Brigadier Alejandro Moressi están y estarán en condiciones de ver la fricción del combate, que el genio militar prusiano dispuso en su libro de la guerra.

**BIBLIOGRAFÍA**


ROB 00-01, R. (2015). Conducción para las Fuerzas Terrestres (Capítulo VII- Sec XV Art 7100). 54-56. Buenos Aires, Buenos Aires, Argentina: Departamento Doctrina.

America, D. o.-t. (8 de junio de 2018). Cyberspace Operations. GL-4 (5-70). Washington DC, United States of America: Joint Publication.

Anca, L. (2015). *La Conducción de Operaciones de Ciberdefensa.* Ciudad Autónoma de Buenos Aires.: TFI, Escuela Superios de Guerra.

Arquilla y Ronfeldt. (2003). *Redes y guerras en red. El futuro del terrorismo, el crimen organizado y el activismo.* Madrid, España: Alianza.

Brett, W. (2011). ten propositions regarding cyberspace operations. *Joint Force Quarterly 61 second quarter*, 11-17.

Cicerchia, C. D. (20 de mayo de 2019). Ingeniero en Sistemas. (C. I. Cabrera, Entrevistador) Buenos Aires.

Corletti Estrada. (2017). *Ciberseguridad, Una Estrategia Informático/Militar.* Madrid, Madrid, España: Recuperado de http://www.darfe.es/joomla/.

Corletti Estrada, A. (2016). *Seguridad en Redes.* Madrid, Madrid, España: Recuperado de http://www.darfe.es/joomla/.

De Vergara y Trama. (2017). *Operaciones Militares Cibernéticas.* (E. S. Armadas, Ed.) Ciudad Autónoma de Buenos Aires, Buenos Aires, Argentina: Visión Conjunta.

Escuela Superior de Guerra Conjunta. (2015). *Arte y Diseño Operacional.* Buenos Aires: Visión Conjunta.

Estrada, A. C. (2011). *Seguridad por Niveles.* madrid, Madrid, España: Recuperado de http://www.darfe.es/joomla/.

Estrada, A. C. (2017). *Ciberseguridad, Una Estrategia Informático/Militar.* Madrid, Madrid, España: Recuperado de http://www.darfe.es/joomla/.

Gniesko, C. I. (2017). *Análisis de las herramientas disponibles para la determinación de un.* Escuela de Guerra Conjunta. CABA: Escuela Superior de Guerra.

Gomez de Agreda, A. (2012). *El ciberespacio. Nuevo escenario de confrontación.* Universidad Politécnica de Madrid. Malaga: Ministerio de Defensa.

Gómez, M. O. (2017). *La resiliencia aplicada al nivel operacional en el ambiente cibernético.* CABA: Escuela Superior de Guerra Conjunta.

Grogovinas, C. A. (2017). *Diseño de un Elemento de Ciberoperaciones en apoyo a la GUB.* Ciudad Autónoma de Buenos Aires.: Escuela Superior de Guerra.

Guimpel, L. A. (24 de mayo de 2019). Oficial de Estado Mayor, Analista de Sistemas. (C. I. CABRERA, Entrevistador) Buenos Aires.

Howard y Paret . (1976). *Clausewitz, Carl von, On War.* Princeton University Press. Nueva Jersey: (Princeton University Press, 1976).

Kaplan, F. (2016). *The secret history of Cyber War.* New York: Simon & Schuster.

Kenny, Locatelli, Zarza. (2015). *Arte y Dideño Operacional.* Ciudad Autónoma de Buenos Aires, Buenos Aires, Argentina: Visión Conjunta.

Llongueras Vicente. (2013). *La Guerra Inexistente, la Ciberguerra. Ciberdefensa.* Saarbruchen, Saarbruchen, Alemania: Académica Española.

Llongueras Vicente, A. (2013). *La Guerra Inexistente, la Ciberguerra. Ciberdefensa.* Saarbruchen, Alemania: Académica Española.

López Hernadez Ardieta, J. (2013.). *Capacidades Esenciales para una Ciberdefensa Nacional.* Panamá: Indra.

López Rosetti. (2019). *Equilibrio.* CABA: planeta.

Lucero, J. (2015). *Ciberdefensa. La dimensión desconocida.* Buenos Aires: Revista Visión Conjunta Nro 12.

Miessler, D. (octubre de 2019). *The Difference Between Red, Blue, and Purple Teams*. Recuperado el 15 de octubre de 2019, de The Difference Between Red, Blue, and Purple Teams: https://danielmiessler.com/study/red-blue-purple-teams/

Ministerio de Defensa de Argentina. (1998). *Diccionario para la Acción Militar Conjunta, RC 00-02.* Buenos Aires: Ministerio de Defensa de Argentina.

Ministerio de Defensa de Argentina. (2014). *Doctrina Básica para la Acción Militar Conjunta, PC-00-01.* Buenos Aires: Ministerio de Defensa de Argentina.

Moliner González, J. (2 de Agosto de 2016). *Instituto Español de Estudios Estratégicos(Varsovia, La cumbre de la OTAN en)*. Obtenido de http://www.ieee.es/Galerias/fichero/docs_opinion/2016/DIEEEO79bis-2016_CumbreOTAN_Varsovia_Moliner.pdf

Moresi, A. (Abril de 2019). *Observatorio Argentino del Ciberespacio*. Recuperado el 3 de mayo de 2019, de http://www.cefadigital.edu.ar/bitstream/123456789/1157/1/2019%2004%20BOLETIN%20OAC.pdf

Nacional, P. E. (2018). *Directiva de Política y Defensa Nacional.* República Argentina, Ministerio de Defensa, CABA.

Nacional, Poder Ejecutivo. (9 de Amyo de 2019). *Directiva Estratégica de Ciberseguridad de la República Argentina.* CABA.

NATO. (2008). *CCDCOE*. Obtenido de Cooperative Cyber Defence Centre of Excellence: https://ccdcoe.org/

PC00-01. (2014). Doctrina Básica para la Acción Militar Conjunta (Estado Mayor Conjunto ). Buenos Aires: Ministerio de Defensa de Argentina.

PC20-01. (2017). Planeamiento para la Acción Militar Conjunta NO. 13-29. Buenos Aires: Ministerio de Defensa de Argentina.

PC20-01. (2017). Planeamiento para la Acción Militar Conjunta, Nivel Operacional (Estado Mayor Conjunto). 13-29, 31-37, 38-54. Buenos Aires, Buenos Aires, Argentina: Ministerio de Defensa de Argentina.

Quinn, J. B. (1980). Estrategias para el cambio. 293-305.

Ramió, C. (2019). *Inteligencia Artificial y Administración Pública.* Madrid: Catarata.

Rio, A. G. (2013). El Ciclo OODA y la toma de decisiones en el Planeamiento. *Trabajo Final Integrador (Planeamiento Operacional)*, 4-13. CABA, Buenos Aires, Argentina: CEFA digital.

ROD05-01. (2016). Conceptos Básicos sobre Sistemas de Comunicaciones, Informática y Guerra Electrónica de la Fuerza(Ejército Argentino). Buenos Aires: Departamento Doctrina (Dirección de Comunicaciones e Informática).

Rosetti, D. L. (2019). *Equilibrio.* (E. Planeta, Ed.) CABA, CABA, Argentina: Planeta.

Salis, E. (2010). *Ethical Hacking.* Buenos Aires: Alfoamega.

Snowden, E. (2019). *Vigilancia Permanente.* Buenos Aires: Planeta.

Stel, E. (2005). *Guerra Cibernética.* Buenos Aires: Círculo Militar.

Teniente Coronel del Ejército de Portugal da Silva Perdigao, H. A. (s.f.). Lod.

Trump, D. (2018). *National Cyber Strategy of the United States of America.* Washington DC, United States of America: The White House.

Uzal, R. (Noviembre de 2015). *http://www.cari.org.ar/pdf/boletin62.pdf*. (C. ". Internacionales", Editor, & ISIAE"Instituto de Seguridaad Internacional y Asuntos Estratégicos ") Recuperado el mayo de 2019, de http://www.cari.org.ar/pdf/boletin62.pdf:

Van Creverd, M. (2007). *La transformación de la Guerra.* (UCEDA, Ed.) Buenos Aires, ARgentina: Reimpresión Buenos Aires. 2007 . UCEDA.

Vargas Vargas, M. (2014). *CIBERSEGURIDAD Y CIBERDEFENSA: ¿QUÉ IMPLICACIONES TIENEN PARA LA.* Bogota: Recuperado de http://repository.unimilitar.edu.co/bitstream/10654/12259/1/CIBERSEGURIDAD%20Y%20CIBERDEFENSA.%20TRABAJO%20DE%20GRADO.pdf.

Vego, M. (2007). *Joint Operational Warfare. Theory and Practise.*

Vergara, D. (2010). El estudio de la historia militar. La evolución del pensamiento estratégico. *Visión Conjunta*.

**Anexo 1 : <u>Entrevista Cnl Daniel Cicerchia 140830May19 (100 minutos)</u>**

1) La ciberdefensa es exclusiva de los militares.
   Responde: No. Si bien la columna vertebral de la ciberdefensa es de los militares, en la actualidad hay muchas organizaciones y universidades que viven y trabajan sobre esta problemática a diario. Por tal motivo, la ciberdefensa debería manejarse de manera holística teniendo en cuenta todas las organizaciones (ejemplo: Israel, Rusia, EEUU y España).

2) Cómo se estructura la ciberdefensa que elementos la componen.
   Responde: Recién en la actualidad se están estableciendo relaciones de Comando entre el Estado Mayor Conjunto y los ámbitos específicos, lo cual limita la preparación y el avance en este dominio debido a cuestiones culturales principalmente. Desde el punto de vista estratégico también hay cosas desnaturalizadas, como por ejemplo la inclusión del Ministerio de Modernización otorgándole las Infraestructuras críticas a ese Ministerio y no a Defensa. No así, como lo desarrolló Brasil, Alemania o Chile que rápidamente entendieron que este dominio necesita tomar decisiones con perentoriedad. Lo cual lo obliga a la Argentina a trabajar en la actualidad de manera reactiva.

3) Como dividiría a las ciberoperaciones. Y cuál es la finalidad de cada una de ellas. (Ofensivas, Defensivas y de Información).
   Responde: En general se dividen en Ofensivas, Defensivas. Lo más importante es entender es que técnicamente quién se defiende bien no sabe atacar y, lo mismo a viceversa. Por esto potencias como Israel tienen divididas las operaciones ofensivas y defensivas en diferentes grupos.

4) Hasta que nivel es conveniente planificar las ciberoperaciones (Nivel Estratégico Nacional, Militar, Operacional, Táctico (BR?)).
   Responde: La ciberdefensa debería planificarse en todos los niveles, sin lugar a dudas, esto permitirá que si bien un nivel como el táctico no disponga de los medios su recurrencia ante la necesidad de lograr algún efecto en el desarrollo de las operaciones. Así mismo, rápidamente se debe dotar en todos los niveles a personal y fracciones capacitados inicialmente para trabajar en este dominio y fomentar el

perfeccionamiento constante ya que el personal que opera en este dominio se debe perfeccionar a diario. Todos los elementos de comunicaciones deberían ser convertidos en elementos de ciberguerra debido a que manejan las redes y tienen la preparación básica para poder explotar este dominio.

5) Las operaciones de información se ejecutan en todo momento.
   Responde: Si, pero son responsabilidad a mi juicio del Área de Inteligencia y utilizan al ciberespacio como medio. Ellas buscan afectar el proceso de toma de decisiones.

6) Qué relación tienen estas con los MCS.
   Responde: Se relacionan con los medios de comunicación social para los cuales la ciberdefensa es un medio.

7) Cuál es la oportunidad para ejecutar ciber operaciones ante un conflicto.
   Responde: Las ciberoperaciones se deben desarrollar en todo momento. Si pensamos en una campaña deberían ejecutarse en todas sus fases y al igual que las comunicaciones o la guerra electrónica comienzan a operar ante del despliegue de las tropas. En la actualidad la ciberdefensa, las comunicaciones y la guerra electrónica son inseparables.

8) Las ciberoperaciones pueden considerarse el CDG de las operaciones. En qué fase?.
   Responde: Piense en un conflicto con intereses económicos, la zona de interés del ciberespacio puede ser el mundo. En el nivel Operacional que se encuentra acotado a un teatro de operaciones determinado, una fuerza cibernética ofensiva puede tener la misma forma de operar que las fuerzas especiales. Sin embargo, la principal diferencia es que esta va a estar constituida por todo tipo de personal incluso muchos civiles que tengan la capacidad de operar en este dominio, las fuerzas especiales utilizan partisanos para operar dentro del dispositivo enemigo. En el ciberespacio es mucho más utilizado pero debe ser bien conducido.
   Por otro lado la conducción de las operaciones en el TO deben ser del Comandante porque él tiene la responsabilidad de llevar a cabo los efectos en las operaciones cuente o no con los medios

8) Cuáles son los principales efectos que buscan las ciberoperaciones.

9) La Percepción de los pueblos o líderes se relacionan con los efectos a producir en las ciberoperaciones.

   Responde: Sin duda es uno de los efectos pero también se relaciona con las operaciones de información

10) La ciberdefensa tiene un departamento que mide la aplicación de los efectos permanentemente.

    Responde: Hoy se encuentra en desarrollo y lo más importante es generar las capacidades iniciales para poder ver efectos en este espacio.

11) Podemos decir que la afectación de la percepción de la población es un efecto importante a cumplir por la ciberdefensa cuando se intenta modificar el proceso de toma de decisiones al más alto nivel.

    Responde: Sin dudas la ciberdefensa es un medio que actuara para modificar el proceso de toma de decisiones.

12) Quien determina o como se determinan los efectos en ciberdefensa.

    Responde: Los efectos los determina el elemento que los ejecuta siempre y cuando se vaya a reconocer como autor del hecho.

13) Podrá responderse a un ataque cibernético de manera cinética

    Responde: Sin dudas ya está ocurriendo, pero nuestro país aún no hay nadie que estudie lo que ocurre en medio oriente y en el mundo

14) Usted cree que la sociedad Argentina perciben las operaciones en las redes como una amenaza.

    Responde: En general No, del 100 por ciento de la población solo un 10 por ciento está informada y conoce las implicancias de este dominio. Compare la historia reciente como por ejemplo Estonia 2007, que pasaría si la sociedad Argentina sufriese un ciberataque de esa magnitud. Que capacidades deberíamos formar para tratar de contrarrestar algo así o defender nuestras estructuras críticas.

15) Como ubicaría a nuestro país desde la conciencia con respecto a la ciberguerra en el contexto mundial.

Responde: Extremadamente bajo. Consulte la cantidad de intromisiones diarias que reciben todos los organismos del Estado o diferentes empresas privadas y podrá corroborar esta afirmación. En general es muy bajo con respecto a los países de la región incluso, como Brasil y Chile.

**Anexo 2: <u>Entrevista al  Cnl Luis Pablo Guimpel 070800Jun19 (100 minutos)</u>**

1. Que es la ciberdefensa

   Responde: Para entender la ciberdefensa es necesario aclarar algunos términos. Hay tres términos que siempre se confunden, seguridad informática, ciberseguridad y ciberdefensa. La seguridad informática es la protección de la triada CID (confiabilidad, integridad y disponibilidad de los datos). Datos: redes informáticas y digitales.

   La ciberseguridad, es una política estratégica nacional que está referido al logro de la protección de las infraestructuras críticas (ICC). Una ICC es una plataforma que provee un servicio esencial para los intereses nacionales. Ejemplo, si yo a traves de un ataque cibernético modifico la fórmula de un medicamento para que sea tóxico puedo llegar a matar gente, si yo rompo los controles de temperatura o presión atmosférica en una central nuclear puedo causar una explosión nuclear como Stuxnet en Irán y matar gente.

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

2. La ciberdefensa es exclusiva de los militares.

   Responde: No. Si bien la columna vertebral de la ciberdefensa es de los militares, en la actualidad los objetivos se cumplen de acuerdo a como son asignados por la Secretaria Nacional de Ciberdefensa.

3. Cómo se estructura la ciberdefensa que elementos la componen.

   Responde: Hay un Comité de Ciberseguridad creado en el ámbito de Modernización, lo integran representantes de todos los ministerios y organizaciones privadas que tienen ICC. La organización para el trabajo de ciberdefensa está dado en dos niveles el CERT y el SOC. El CERT está distribuido en todas las organizaciones y después cada organismos tiene su SOC que es el centro de operaciones. Las ordenes y efectos a lograr  los establece el Poder Ejecutivo, en la actualidad se están desarrollando capacidades y nuestros SOC trabajan diariamente con más de 1000 intrusiones diarias.

4. Como dividiría a las ciberoperaciones. Y cuál es la finalidad de cada una de ellas. (Ofensivas, Defensivas y de Información).

Responde: En general se dividen en Ofensivas, Defensivas y de Exploración. Lo más importante es entender es que técnicamente quién se defiende bien debe desarrollar su capacidad para atacar. Esto va a depender del nivel de los actores, solo los actores de nivel 3 poseen los recursos para sostener un ciberataque en el tiempo. Los actores de nivel 1 y 2 son fáciles de bloquear.

5. Hasta que nivel es conveniente planificar las ciberoperaciones (Nivel Estratégico Nacional, Militar, Operacional, Táctico (BR?)).
   Responde: La ciberdefensa debería planificarse en todos los niveles pero el mayor detalle en este caso lo tendrá el nivel estratégico. Sin embargo debe planificarse hasta el nivel Unidad Táctica.

6. Las operaciones de información se ejecutan en todo momento.
   Responde: Si, son permanentes. Ellas buscan afectar el proceso de toma de decisiones. Hemos tenido muchos intentos de intrusión en el comando electoral, durante el G20 y permanentemente en las redes que controla el Comando Conjunto de Ciberdefensa con los CERT(s) Y SOC(s).

7. Qué relación tienen estas con los MCS.
   Responde: Todos ya que las mismas planifican efectos para ser ejecutados en gran parte con los medios de comunicación social, en el cual la ciberdefensa es un medio.

8. Cuál es la oportunidad para ejecutar ciberoperaciones ante un conflicto.
   Responde: Las ciberoperaciones se deben desarrollar en todo momento. Si pensamos en una campaña deberían ejecutarse en todas sus fases y al igual que las comunicaciones, estas se deben ejecutar en todas las capas del ciberespacio. La ciberdefensa, la guerra electrónica y las comunicaciones son inseparables en la actualidad.

9. Las ciberoperaciones pueden considerarse el CDG de las operaciones. En qué fase?.
   Responde: Pensando en los tres grandes conflictos Estonia, Georgia y Ucrania. Luego de estonia 2007 la OTAN estableció que cualquier ciberataque es considerado un acto de guerra, por este motivo los potencias intentan no atribuirse los

ciberataques que ejecutan permanentemente. Si suponemos que Rusia estableció un plan de campaña para atacar a la nación más digitalizada del mundo en Estonia 2007, sin dudas la ciberdefensa fue el CDG. Ahora yendo a Georgia donde Rusia si se atribuyó el ciberataque Rusia durante una semana logro paralizar a ese país dejándolo sin comando y control y una vez frenado este invadió con tropas convencionales, ahí no es el CDG la ciberdefensa, habrá sido el CDG de esa fase. En esa fase el CDG fue ciberdefensa. En ucrania el ataque cibernético se hizo con tropas, EEUU divide al ciberespacio en tres capas. Una capa física, una capa lógica y una capa social siempre y cuando los objetivos se dirijan contra un backbone o cualquier. Las ciberoperaciones pueden ser el CDG dependiendo de la campaña. En una guerra convencional el CDG no es la ciberdefensa, pero el mundo hoy no está viviendo ese tipo de conflictos.

Todo va a depender también de cual sea el objetivo estratégico nacional para determinar si la ciberdefensa puede ser o no el CDG de la campaña.

10. Cuáles son los principales efectos que buscan las ciberoperaciones.

    Responde: del tipo de ciberoperacion a ejecutar. Las ciberoperaciones ofensivas por lo general tienen efectos de neutralizar o manipular mientras que el principal efecto de las ciberoperaciones defensivas es proteger.

11. La Percepción de los pueblos o líderes se relacionan con los efectos a producir en las ciberoperaciones.

    Responde: Sin duda es uno de los efectos más importantes que intentara modificar el proceso de toma de decisiones.

12. La ciberdefensa tiene un departamento que mide la aplicación de los efectos permanentemente.

    Responde: Si tenemos ya que el Comando conjunto de Ciberdefensa funciona como cualquier Unidad. Hoy se encuentra en desarrollo y lo más importante es generar las capacidades iniciales para poder ver efectos en este espacio.

13. Podemos decir que la afectación de la percepción de la población es un efecto importante a cumplir por la ciberdefensa cuando se intenta modificar el proceso de toma de decisiones al más alto nivel.

Responde: Sin dudas las ciberoperaciones son un medio que actúan para producir efectos sobre la población, sino estudiemos los conflictos como Estonia, Ucrania y Georgia si uno de los actores no generó las condiciones sobre la población para inclinar los conflictos a su favor.

14. Quien determina o como se determinan los efectos en ciberdefensa.

Responde: Los efectos los determina el Poder Ejecutivo por medio de la Secretaria de Ciberdefensa.

15. Podrá responderse a un ataque cibernético de manera cinética

Responde: Sin dudas ya está ocurriendo, pero nuestro país aún no tiene desarrollado en forma completa el marco legal. Sin embargo la OTAN y el manual de Tallin lo establecen.

16. Usted cree que la sociedad Argentina perciben las operaciones en las redes como una amenaza.

Responde: En general No, la sociedad Argentina es extremadamente crédula.

17. Como ubicaría a nuestro país desde la conciencia con respecto a la ciberguerra en el contexto mundial.

Responde: Bajo. Pero estamos desarrollando las capacidades para estar a la altura de los países de la región como Brasil.