MATERIA: TRABAJO FINAL INTEGRADOR

TEMA:

GUERRA CIBERNETICA Y DISEÑO OPERACIONAL

TÍTULO:

LA GUERRA CIBERNETICA EN EL ARTE Y DISEÑO OPERACIONAL

AUTOR: My ENCINA, Guillermo Antonio

Año 2019

RESUMEN

Los conflictos de la actualidad hacen un empleo intensivo del dominio correspondiente al ciberespacio, donde los límites están dados por el pensamiento como teatro de operaciones. En dicho espacio no se distinguen combatientes y no combatientes, y este escenario se presenta con mayor complejidad, con una necesidad de una toma de decisiones más rápida y un planeamiento acorde.

En este trabajo se estudia, teniendo como eje central el efecto que tendrán las operaciones de la guerra cibernética en los elementos del diseño operacional, siendo este el objetivo principal de la investigación, de manera tal de establecer un aporte académico que resulte una herramienta contribuyente al arte y diseño del nivel operacional para el comandante y su órgano de planeamiento.

Como resultado de este trabajo final integrador se obtiene que el grado de influencia que tienen las operaciones de guerra cibernética sobre los elementos del diseño operacional, donde se desprende que implican una adaptación en algunos de esos elementos del diseño operacional. Si bien no es un cambio esencial, es necesaria una visión particularizada, a los efectos de lograr un diseño integral enfocado en una línea de operaciones que le sea propia.

La idea es presentar una lectura amena, sencilla, enfocada a quienes buscan iniciarse en ambas temáticas con conceptos claros y redefinidos por el autor luego de un profundo análisis de los elementos del diseño operacional. De igual manera con los conceptos correspondientes al ciberespacio, los medios informáticos y la relación existente entre éstos y la herramienta de planeamiento que tiene el nivel operacional.

Muchos de los conceptos aquí vertidos surgieron de las clases del Curso Introductorio Avanzado en la Ciberdefensa y la Ciberseguridad, que es impartido, como parte de la extensión universitaria de la Escuela Superior de Guerra Conjunta.

Palabras clave: Elementos del Diseño Operacional, Guerra Cibernética, Ciberespacio, Ciberdefensa, Ciberamenazas.

TABLA DE CONTENIDOS

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

INTRODUCCIÓN

Este trabajo final tiene como objetivo general determinar el grado de influencia que tiene la guerra cibernética sobre los elementos del diseño operacional, con la intención de establecer en qué medida se ven afectados estás herramientas del arte y diseño operacional.

Si bien ambos conceptos no son nuevos y existen muchos trabajos referidos. En esta investigación se tratará de dar una visión estableciendo un lenguaje de uso común, ya que existe una gran variedad de conceptos y definiciones. Por lo tanto, es necesario a los efectos de esta investigación, adaptar conceptos en primer término y luego asociarlos para arribar a una conclusión de interés.

Es destacable el trabajo realizado por Sergio Sepetich bajo el título *Las ciberoperaciones aplicadas a un Teatro de Operaciones-estudio de caso: Guerra Ruso Georgiana* en el marco de la Guerra Ruso-Georgiana del año 2008. Aquí, el autor desarrolla definiciones generales de las ciberoperaciones en el nivel operacional, las cuales son importantes por ser conceptos iniciales a esta investigación y resulta de sustancial interés para contar con un lenguaje común.

En el mismo sentido, Ezequiel Rodríguez Cisneros, en su trabajo *Desafíos operacionales en el ciberespacio como nuevo campo de lucha*, brinda el marco legal nacional e internacional y las ambigüedades existentes en la definición de ciberespacio en la Argentina.

Por otro lado, el trabajo final de investigación de Augusto Rivolta, *Las vulnerabilidades de las operaciones militares derivadas de las redes sociales en internet*, desarrolla conceptos sobre la ciberguerra, el análisis de la situación y su relación con las fortalezas, oportunidades, debilidades y amenazas, aspectos que servirán para determinar qué tipo de operaciones se tendrán en cuenta para esta investigación.

Otro antecedente a tener en cuenta es el de Juan Barbosa Larronde, *Dificultades para la obtención de la sorpresa en el nivel operacional ante el avance de nuevas tecnologías de la información*. En el desarrolla los sensores activos y pasivos, y las operaciones necesarias de velo y engaño para obtener la sorpresa en el nivel operacional, aspectos que se tendrán en consideración para esta investigación.Por su parte, Daniel Giudici, en *Lineamientos para la seguridad cibernética en el teatro de operaciones*, analiza los tipos de amenazas y aquellas acciones defensivas y la necesidad de capacitar especialistas.

Eduardo Páez, enfoca su trabajo, *La guerra cibernética en el nivel operacional*, en las capacidades de ciberguerra de cada una de las fuerzas armadas, las características que debe poseer el soldado ciberguerrero, y una idea de un comando conjunto de ciberdefensa.

En líneas generales, estos aportes destacan una variedad de definiciones actualizadas respecto de la guerra cibernética. En todos los casos se remarca la importancia que se debe dar a su conocimiento y aplicación en el nivel operacional, aunque no se ha profundizado en un análisis sobre cada uno de los elementos del diseño operacional bajo la influencia de las operaciones en el marco de la guerra cibernética. Evergisto de Vergara y Gustavo Trama, en el texto *Operaciones militares cibernéticas: Planeamiento y Ejecución en el Nivel Operacional*, abordan en forma detallada algunos de los elementos del diseño operacional en relación con la guerra cibernética, con extractos de varios autores extranjeros. En tal sentido, Gustavo Trama en *Operaciones Cibernéticas: su naturaleza, propósito y conducción*, concluye a modo de pregunta cuál es la forma en que el comandante operacional debería incluir las operaciones cibernéticas en el planeamiento de nivel operacional.La *Guerra cibernética* de Enrique Stel presenta un análisis de ataques cibernéticos y los aspectos y vacíos legales nacionales e internacionales que son de vital importancia para la presente investigación al asociar estos ejemplos históricos con las anteriores definiciones.

Conceptos, definiciones y estudio de casos que se desarrollan en estos antecedentes sirven de marco conceptual para la presente investigación.

El estado actual del tema sugiere analizar en profundidad cada elemento del diseño operacional y la influencia de la ciberguerra sobre ellos, a fin de determinar que parámetros se deberían adoptar como criterio o factor de planeamiento, si es que existen.

En concordancia con lo expuesto precedentemente, el problema de investigación es ¿cuál es la influencia de la guerra cibernética en los elementos del diseño operacional?

El alcance de esta investigación incluye el análisis detallado de cada elemento del diseño operacional y su relación con la guerra cibernética. Dentro de este marco, se analiza consideraciones que puedan definir usos de carácter ofensivos y de protección de propias fuerzas dentro del diseño operacional.

Contrariamente, quedan excluidos del análisis aquellos conceptos referidos a aspectos legales vigentes dentro del marco nacional o del derecho internacional de los conflictos armados. Se toma como guía la bibliografía obligatoria de la Escuela Superior de Guerra Conjunta en lo referido a los elementos del diseño operacional, de acuerdo a la clasificación en elementos tradicionales del diseño operacional, elementos innovadores del diseño operacional y elementos circunstanciales del diseño operacional.

El estudio se centra en la planificación y el diseño operacional y no se analizan impactos en las áreas específicas de personal o de material. No obstante, no se estudian ni proponen

principios de la guerra en relación a los elementos del diseño operacional y las operaciones de guerra cibernética, como tampoco, se propone una fuerza cibernética, sus misiones, funciones, concepto de empleo ni elementos de comando específicos o conjuntos.

Las conclusiones finales del presente trabajo tienen por objetivo establecer cuáles son los mínimos parámetros al momento de diseñar la campaña teniendo en cuenta la influencia de la guerra cibernética en cada uno de los elementos del diseño operacional, si los hubiere y en qué grado.

Este trabajo podría resultar de utilidad y de necesario tratamiento en las materias relacionadas con el planeamiento de operaciones militares al tratar de crear la consciencia de incluir ésta temática como de vital importancia, sobre todo en el nivel operacional de la guerra.

La hipótesis sugiere que las operaciones que comprenden la guerra cibernética tendrían influencia en los elementos del diseño operacional y esto implicaría saber en qué grado impactará sobre cada elemento del diseño operacional y, en base a estos conocimientos, quienes tengan la responsabilidad de diseñar la campaña adoptarán las previsiones necesarias para proteger de estas amenazas sus propias organizaciones militares y no militares, infraestructuras, instituciones gubernamentales y no gubernamentales.

En este diseño operacional de la campaña se utilizarán estas operaciones de guerra cibernética en conjunción con los elementos del diseño operacional para contribuir con el logro del objetivo operacional y con el disloque del centro de gravedad del oponente.

La presente investigación implica una metodología cualitativa con un diseño descriptivo en el que se emplean fuentes primarias y secundarias, entre ellas análisis textos bibliográficos, reglamentos, trabajos de investigación, otros documentos, páginas de internet de grado confiables para el trabajo. Se tendrán en cuenta las fuentes nacionales y extranjeras que sean afines a la temática en orden temporal longitudinal.

Como se indicó, el trabajo tiene como objetivo general determinar el grado de influencia que tiene la guerra cibernética sobre los elementos del diseño operacional y se estructura en dos capítulos analíticos. El primer capítulo tiene como objetivo particular seleccionar aquellos elementos del diseño operacional que de alguna forma pueden verse influenciados por la guerra cibernética.

Mientras que en el segundo capítulo se plantea como objetivo particular identificar el efecto que producen las acciones de la guerra cibernética y que pueden influir en los elementos del diseño operacional.

Finalmente, se presenta la conclusión en lo referido a la relación que tienen ambos conceptos y que permite responder la hipótesis del trabajo final integrador.

CAPÍTULO 1. Los Elementos del Diseño Operacional

En este capítulo se analizan aquellos elementos del diseño operacional que pueden ser influenciados por las operaciones cibernéticas. En primer lugar, se debe dejar claro que son los elementos del diseño operacional, ya que el reglamento *Planeamiento para la acción Militar Conjunta (PC 20 – 01)* lo define utilizando la misma palabra, *son elementos*, por lo cual es más apropiado, que para una correcta interpretación, que son *herramientas* útiles que se destinan a la creación de un concepto operacional.

1.1 Elementos Tradicionales del Diseño Operacional

1.1.1 Objetivo

El objetivo es aquel objeto material o inmaterial que, al ser conseguido, puede materializar la concreción del estado final deseado operacional (EFDO), aunque no necesariamente. Se requiere que el objetivo sea claro, definido y decisivo pudiendo existir más de un objetivo. Por lo tanto, se buscará priorizarlos siendo el último el que reunirá las condiciones de objetivo operacional.

Entonces, en el párrafo anterior queda de manifiesto el valor que debe poseer este EDO, por lo cual las acciones de ciberguerra deberán estar dirigidas hacia un objetivo cibernético claro, decisivo y alcanzable dentro de una línea de operaciones propia (LO).

Cuando se deba elegir el objetivo cibernético que será atacado, se debe tener en cuenta que no regirá para éste el Principio de Distinción, porque el ataque con vectores cibernéticos no hace la distinción pertinente entre objetivos militares y civiles o bienes protegidos.

El párrafo precedente marca una diferencia importante entre objetivo cibernético y el objetivo militar tradicional, por lo tanto su elección debe ser considerada con un alto grado de exactitud.

1.1.2 Niebla

La complejidad que caracteriza a los conflictos actuales está dada, en gran medida, por la velocidad en las acciones y la mayor incertidumbre que presenta el ambiente operacional. En el ciberespacio esta incertidumbre es igual o mayor, ya que entran en juego definiciones

propias de este dominio como la Ciber-atribución, la Ciber-anonimidad y la Ciber-disuasión, que se desarrollan en el siguiente capítulo.

Entonces, es posible adaptar el concepto de Carl Von Clausewitz y hablar de Ciberniebla de la guerra, como todas aquellas ciberoperaciones que realiza un oponente y afecta las propias operaciones, donde existe una mayor complejidad por la cantidad y variedad de posibles actores, donde se incluyen hacktivistas, terrorismo, crimen organizado, otro tipos de atacantes y, por supuesto, el gobierno al cual pertenece el oponente.

Estos son como nuevos ingredientes en este escenario que plantea el quinto dominio de la guerra, el ciberespacio.

1.1.3 Fricción

Cobra suma importancia el concepto de fricción, ya que en este nuevo ambiente operacional se deberán incrementar las medidas de seguridad, de contrainteligencia, y todo otro proceso que implique el uso de medios cibernéticos por parte de todos los actores intervinientes, combatientes y no combatientes quienes podrán provocar un aumento significativo en la ciber niebla de la guerra.

Se entiende, entonces por fricción a todas aquellas actividades de carácter informático que se realicen desde el propio bando y que su mal empleo por negligencia, descuido, falta de instrucción entorpezcan las propias operaciones.

En este concepto se engloban a aquellos actores de la propia organización que representan, por lo tanto, una amenaza de carácter interno, como ser soldados con poca instrucción, que colaboran con el oponente por alguna razón, de igual manera esta situación se puede manifestar en el proveedor del servicio o administradores de red, entre otros.

1.2 Elementos Innovadores del Diseño Operacional

1.2.1 Estado Final Deseado Operacional

Este elemento del diseño operacional implica una modificación de la realidad, como efecto deseado, buscando obtener una situación favorable al dar por terminadas las operaciones militares dentro del teatro de operaciones.

Es importante destacar que el teatro de operaciones implica una porción de territorio ya sea propio, del enemigo o ambas, que será establecido por el poder político y con criterios de finalización para el estado final deseado operacional.

Dentro de estos límites, se encontrará el objetivo operacional que, una vez alcanzado, materializará la consecución del estado final deseado operacional.

En el ambiente del ciberespacio, los límites no podrán ser definidos con claridad, por lo tanto, el concepto de teatro de operaciones se desdibujará en el sentido de la territorialidad, sabiendo que el ciberataque podrá surgir de cualquier punto del planeta.

No son aplicables los conceptos tradicionales de frente, flanco, ala, retaguardia. El ciberataque puede estar dentro del propio territorio, dentro de la propia organización.

Por lo expuesto precedentemente, el estado final deseado operacional será afectado sin dudas por las acciones de la guerra cibernética.

1.2.2 El Centro de Gravedad

Este elemento del diseño operacional es el que más variantes tiene en cuanto a su conceptualización o definición; no existe una definición uniforme en las fuentes doctrinarias ni académicas.

El autor de este trabajo considera que se debería contar con una definición concreta, clara que no genere confusiones o una libre interpretación, que la definición del diagnóstico sea única, aunque su tratamiento pueda variar de acuerdo al conocimiento científico sumado a las habilidades artísticas de quien deba tomar la decisión, en este caso el comandante del nivel operacional de la conducción.

Por un lado, el centro de gravedad es definido por el PC 20 – 01 como fuentes de poder, que proveen fortalezas o capacidades esenciales para el cumplimiento de una misión, que son subsistemas críticos que van a posibilitar al comandante el principio de libertad de acción y voluntad de lucha, diciendo que, el centro de gravedad puede ser de carácter físico o bien puede ser abstracto.

Por otro lado, en el Arte y Diseño Operacional, aborda la definición del centro de gravedad como el ente con capacidad inherente de cumplir con la misión impuesta, y lo va a caracterizar al decir que es de índole material o concreta, descartando a priori que pueda ser de carácter abstracto en este nivel de la conducción.

Hay quienes afirman que es la misma definición del Schwerkpunt, concepto que pertenece a Karl von Clausewitz, en su libro De la Guerra.

Esta variedad de definiciones atenta contra la exactitud necesaria para relacionarlos convenientemente con las actividades de ciberoperaciones. Es por ello que, el autor lo abordará desde un punto de vista sistémico, de forma tal que esta interpretación se pone en mejor perspectiva para ser relacionada con conceptos que hacen a la seguridad informática.

Ante un conflicto, básicamente, nos encontramos ante el choque de dos sistemas, en donde uno de ellos intenta imponer su voluntad sobre el sistema en oposición, pero no necesariamente busca su destrucción total, si no que uno puede desarticular al otro, atacando aquellos puntos vulnerables que generen un efecto disruptivo y que le provoque el colapso afectando su equilibrio sistémico.

Haciendo una analogía con el *Jet Kune Do*, arte marcial creado por Bruce Lee, algunas de sus características de esta forma de lucha incluyen, que primero su creador era de estructura pequeña, evidenciando así una asimetría con otros oponentes más grandes y fuertes.

Sus golpes debían ser precisos a lugares vulnerables que desestabilicen rápidamente al contrincante y evitando así el consumo de energía propio.

Segundo, que esta técnica no tenía reglas fijas, sino que se adaptaba a cada persona y debía evolucionar con nuevas formas, pero manteniendo su esencia de terminar la pelea lo antes posible.

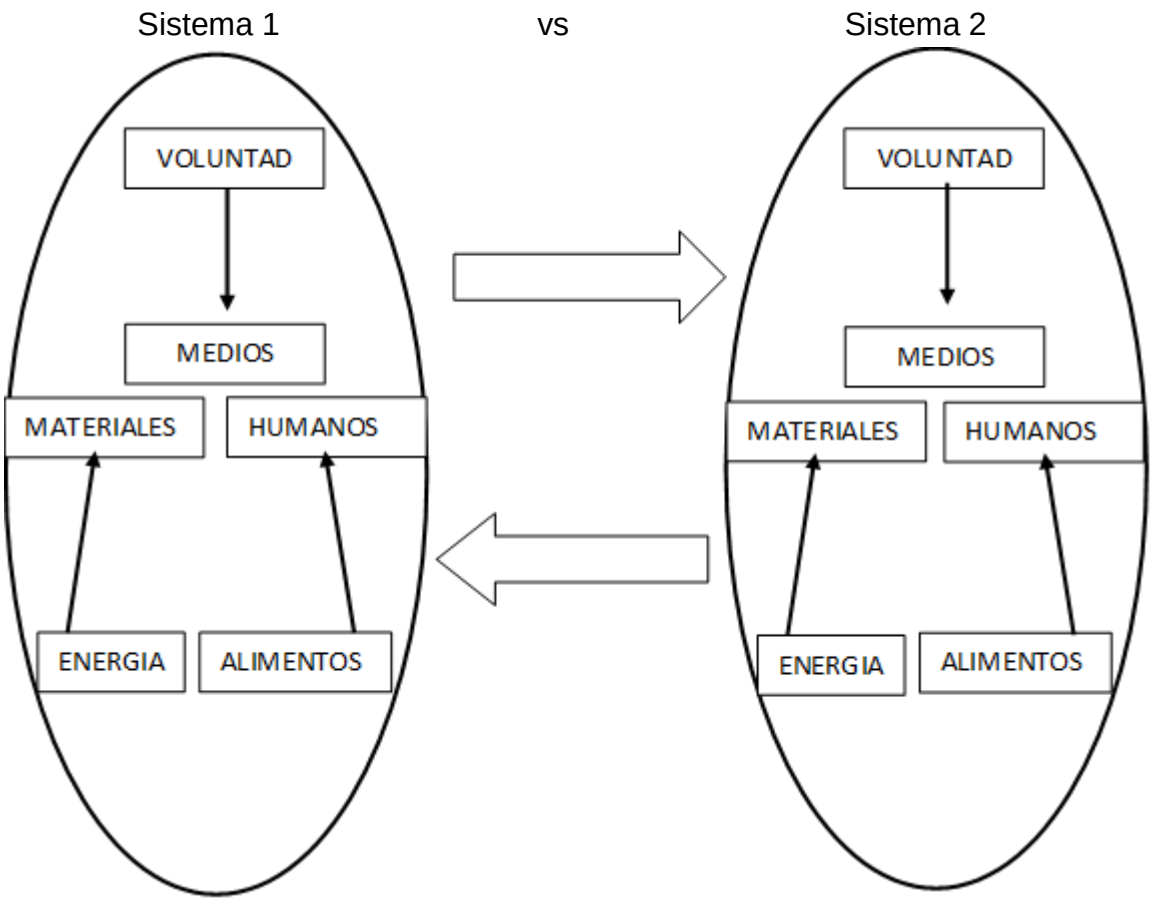
Ahora bien, el decisor de cada sistema necesita saber que sucede en su entorno y, con los pocos datos que tiene, adoptar una decisión acertada decisión y suponer qué va a suceder en el futuro, tratando de modificarlo para alcanzar el estado final deseado. Ésta necesidad de saber lo máximo posible en el menor tiempo, va a caracterizar el uso de la información.

Es en este punto donde aparecen las operaciones cibernéticas tratando de incidir a favor de quien emplea la información, protegiéndola y tratar de afectar el uso de la información por parte del sistema oponente.

A través de ciberataques intenta afectar el subsistema que genere un desequilibrio sistémico disruptivo y con este disloque llevarlo a su punto culminante, que normalmente se encontraran en las infraestructuras críticas, lugares donde se originan o se almacenan la información a modo de datos.

En la figura 1 se muestran dos sistemas en oposición, algún subsistema componente podría llegar el centro de gravedad, de acuerdo a una situación particular.

Figura 1: Sistemas en oposición.

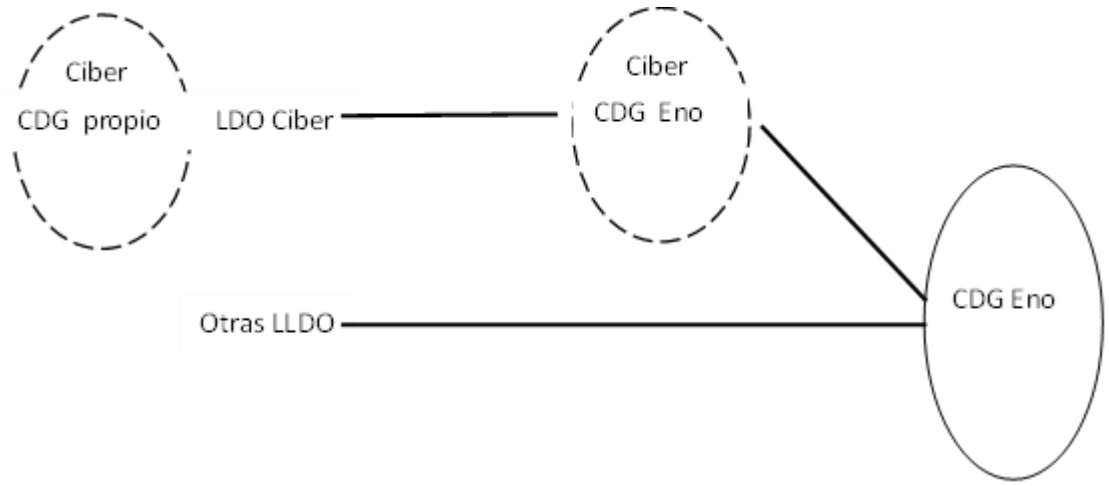


Fuente: elaboración propia.

Esta forma sistémica de ver al centro de gravedad cibernético, implica que dentro del planeamiento general que se efectúa en el nivel operacional y utilizando como herramienta los elementos del diseño operacional, la necesidad de una línea de operaciones propia.

Esta línea de operaciones se transforma en la línea de operaciones cibernética que unirá los puntos decisivos inherentes a este dominio, hasta alcanzar el centro de gravedad cibernético del oponente, será contribuyente al logro del centro de gravedad del oponente, en el cual convergerán todas las otras líneas de operaciones restantes.

Figura 2: CDG Cibernético.



Fuente: elaboración propia.

La determinación del centro de gravedad cibernético en el nivel operacional comprende la búsqueda de la infraestructura crítica esencial.

Las infraestructuras críticas podrán ser asignadas por el nivel estratégico militar quién determina los efectos necesarios a lograr.

Finalmente la ejecución de las acciones para lograr los efectos perseguidos, es responsabilidad del nivel táctico de la conducción.

Es decir que el nivel estratégico militar formula el efecto necesario y asigna las infraestructuras críticas, el nivel operacional determina el centro de gravedad cibernético sobre la infraestructura critica esencial, mientras que en el nivel táctico será establecerla forma en que los subsistemas de armas o de comando y control podrán ser afectados.

En la figura número 2, en donde se presenta un modelo de centro de gravedad cibernético (CDG Ciber). Estos centros de gravedad aparecen en línea discontinua y en forma de anillo, para visualizar que el CDG Ciber está protegido por diferentes capas concéntricas.

Cada uno de estos anillos protectores son capas porosas, o sea deja la firme idea de que ningún sistema, y en este caso, ningún centro de gravedad cibernético es invulnerable.

1.2.3 Líneas de operaciones

Desde el punto de vista cibernético, las líneas de operaciones deben partir desde el centro de gravedad cibernético propio para alcanzar el centro de gravedad cibernético del oponente y así contribuir con el disloque del centro de gravedad del oponente.

Estas líneas de operaciones serán mixtas necesariamente, es decir, físicas porque parten desde un hardware y se unirán a otros (Puntos Decisivos) en forma lógica a través de datos binarios. Desde el punto de vista de la conducción de las operaciones las líneas de operaciones cibernéticas (LO Ciber) tienen un responsable que, junto a una organización adecuada, llámese departamento C VI, (Comunicaciones, Guerra electrónica y Ciberdefensa) las diseñen y conduzcan.

1.3 Elementos Circunstanciales del Diseño Operacional

1.3. 1 Momentum

Cuando se refiere a este elemento del diseño operacional, se habla de la oportunidad en que el comandante operacional considera que es necesario realizar una determinada acción y lograr un efecto.

En el dominio donde se lleva a cabo la ciberguerra, es necesario mucho tiempo de preparación para generar las condiciones favorables a la hora de decidir el momentum.

La falta de adecuada preparación para la guerra hace que victoria o la derrota se dé mucho de tiempo antes de que la guerra empiece, esto es totalmente aplicable a la ciberguerra.

Es necesaria una evolución permanente en los medios tecnológicos, personal permanentemente capacitado y un pre posicionamiento estratégico que incluye ingeniería social y actividades exploratorias de probables oponente.

Lo expresado precedentemente, genera las condiciones necesarias para poder estar a la altura de un oponente que emplee sus instrumentos correspondientes al quinto dominio.

1.3.2 Ritmo

Este elemento del diseño operacional hace referencia a la necesidad de mantener al oponente permanentemente presionado, pero en el ciberespacio esto se traduce en acciones que viajan a la velocidad de la luz. Por lo tanto, se necesitan mentes ágiles, capacitadas y entrenadas, ya

que la velocidad del pensamiento es mayor al de la luz. Esta la forma que se debe entender este elemento del diseño operacional, al momento de pensar en términos de *tiempo, espacio, masa y efecto*.

1.3.3 Punto culminante

La guerra cibernética puede contribuir a que el oponente llegue a su punto culminante. Desde el aspecto meramente cibernético, será muy difícil comprobar si un sistema alcanza un punto culminante en forma permanente o por periodos muy prolongados, ya que seguramente tendrán los medios redundantes necesarios para volver a equilibrar su sistema.

1.3.4 Conclusión parcial del primer capítulo

En el presente capítulo, se han tratado aquellos elementos del diseño operacional que el autor considera necesarios para el arte y diseño operacional en el dominio del ciberespacio.

El trabajo efectuado consistió en analizar y, como resultado de ello, adecuar los distintos elementos del diseño operacional para volcarlos en una línea de operaciones cibernética que facilite visualizar una solución al utilizar técnicas ofensivas o bien técnicas defensivas cibernéticas en relación al propio centro de gravedad o del oponente.

Es importante recordar en este punto que los elementos del diseño operacional son herramientas que forman parte de un método de planeamiento, en este caso, del planeamiento de nivel operacional.

Es decir que, una vez conocido el método de planeamiento y el uso de estas herramientas, éstas pueden ser adaptadas para lograr la posible mejor solución del problema militar operativo en relación con las operaciones cibernéticas.

En la figura 3 y a modo de conclusión se presenta un cuadro con aquellos elementos del diseño operacional tenidos en cuenta para el trabajo de este primer capítulo,

Tabla 1. Cuadro de elementos del diseño operacional.

EDO TRADICIONALES	**GUERRACIBERNETICA**
Objetivo operacional	SI
Esfuerzo operacional	--
Maniobra operacional	--
Niebla	SI
Fricción	SI
EDO INNOVADORES	
Estado final deseado	SI
Centro de gravedad	SI
Puntos decisivos	SI
Líneas de operaciones	SI
EDO CIRCUNSTANCIALES	
Momentum	SI
Tempo o Ritmo	SI
Punto culminante	SI
Alcance operacional	--
Pausa operacional	--
Enlace operacional	--

Fuente: Elaboración propia según *Arte y diseño operacional*, capítulos IV, V y VII.

CAPÍTULO 2. Operaciones de Guerra Cibernética

En el presente capítulo se darán algunas definiciones a tener en cuenta como ser, los elementos componentes de una arquitectura de red, cuáles son las armas cibernéticas más conocidas, otras definiciones necesarias y, finalmente, como se relacionan estas con los elementos del diseño operacional.

2.1 Infraestructura de red

La infraestructura de redes se arma para permitir una comunicación, en este caso, el envío de paquetes de datos de un sistema a otro. La información que allí transita debe poseer las siguientes características: confidencialidad, integralidad, disponibilidad.

La infraestructura de red debe ser diseñada de forma tal que posibilite una eficiente protección, ya que este entramado de cables y dispositivos electrónicos se encontrara el centro de gravedad propio.

Saber diagramar una infraestructura sólida, y sabiendo que es factible de ser vulnerada, son los primeros pasos a tener en cuenta por el defensor, para diseñar un modelo de ataque a la infraestructura de red de un oponente. Por esta razón se expresan los dispositivos componentes de una posible arquitectura de red.

2.1.1 Computadoras

Las computadoras son las maquinas que nos permiten hacer y almacenar datos de todo tipo, como ser textos, planillas, cuadros, gráficos, fotos, videos y que, al conectarlas a un servidor, posibilitan tener acceso a internet. La computadora se transforma así en uno de los lugares más vulnerables de la arquitectura de redes ya que esta interactuando en forma directa con el eslabón más débil de todo sistema, el hombre.

Desde que el usuario establece la conexión a internet, es cuando corre el máximo riesgo de un ataque cibernético y sin saberlo. Es menester que en el ámbito de la ciberdefensa los operadores de las computadoras utilicen las misma en un adecuado marco de conciencia por las medidas de seguridad de informática y de contrainteligencia.

2.1.2 Telefonía celular

En el caso de la telefonía celular, la información viaja por el aire, hacia y desde las torres de antenas celulares y en este trayecto son altamente vulnerables. Otra importante vulnerabilidad es el uso de las aplicaciones que facilitan el uso de la telefonía, muchas de estas aplicaciones revelan la geolocalización del usuario, ya sea en tiempo real o por futuros análisis de ciber forencia

Cada vez que un usuario de telefonía celular enciende su móvil y entra a una aplicación, está reportando el lugar donde se encuentra, donde estuvo y el recorrido que transita a las empresas prestadoras de Google, Facebook, WhatsApp, en Estados Unidos, y también a las empresas prestadoras de servicio celular en el país.

Esto es particularmente importante porque los datos pueden ser obtenidos o capturados del ciberespacio y con la adecuada inteligencia de esa información conseguir valiosos elementos de juicio para ser aplicados en un modelo de diseño operacional para alcanzar un centro de gravedad cibernético.

La telefonía celular representa una considerable debilidad, ya que en el teatro de operaciones habrá miles de estos dispositivos que no estarán bajo control propio y se debe establecer unas instrucciones de comunicaciones particularizadas a tal fin y que permitan un efectivo control a los efectos de minimizar posibles ciberataques.

2.1.3 Servidores

Los servidores son computadoras de gran rendimiento que se utilizan dentro de una arquitectura de red para almacenar información. Estos dispositivos permiten el acceso a internet desde las computadoras y es por esta razón que son objetivos codiciados y por el contenido que se encuentran allí disponibles.

Quien tenga a su cargo el diseño de una arquitectura de red busca la adecuada protección de sus servidores, a los efectos de minimizar los efectos dañinos en caso de que la amenaza cibernética se haga realidad.

2.1.4 Switch

El switch es un dispositivo físico que posibilita el tráfico de datos dentro de una red local. Generalmente conectan computadoras, impresoras, televisor, o algún otro dispositivo que se

quiere que forme parte de esa red. El switch trabaja leyendo las placas de red, conocidas como MAC, y direcciona el tráfico de red hacia sus destinatarios.

2.1.5 Routers

Los routers son dispositivos físicos que se utilizan para conectar segmentos de red y tener un mayor control del tráfico de datos entre ambos. Así como los switch trabajan en base a las placas de red, los routers emplean las direcciones IP, y se los utilizan para mayores prestaciones que incluyen la interconexión con redes de mayor volumen.

El router es un punto de acceso para quienes intenten un ciberataque a través de virus informáticos como el VPN Filter que ha infectado medio millón de estos dispositivos o el Roaming Mantis cuyo propósito es robar información sobre el usuario.

Surge la Medidas preventivas para proteger estos dispositivos incluyen cambiar la contraseña por defecto, utilizar contraseñas robustas para el empleo en wifi, entre otros.

2.1.6 Líneas físicas

Las líneas físicas constituyen los distintos tipos de cableado que unen dispositivos y permiten la transmisión de los datos a grandes distancias. Los proveedores de internet utilizan las líneas físicas para permitir el acceso a los distintos usuarios. Un gran volumen se encuentra en el fondo de los océanos para unir los continentes y están constituido por fibra óptica.

En algunas fuentes de información se menciona que las potencias mundiales como ser Estados Unidos y Rusia hacen inteligencia sobre los puntos de conexión en la fibra óptica con mini submarinos especiales.

Existen una variedad de líneas físicas como ser el cable coaxil, cable UTP entre otros. Al conectar los dispositivos por medio de estos enlaces, hacen de esa estructura un poco más segura que las redes interconectadas por medio aéreo como ser los enlaces de wifi.

Las líneas físicas pueden ser objetivos a ser destruidos a través de ataques cinéticos, o bien pueden ser cortados en forma preventiva para eludir o contrarrestar ataques no cinéticos.

2.1.7 Sistemas operativos

Son protocolos básicos que permiten el funcionamiento de la computadora. Se ejecutan en forma prioritaria y también son llamados núcleos o kernels. Entre los más conocidos se destacan el Windows, el Linux, DOS.

Los sistemas operativos son blancos de las amenazas cibernéticas, ya que existen virus que infectan las computadoras, llamados virus de boot, cuando se enciende y el sistema operativo se carga. En la tabla 2 se observa la clasificación de los sistemas operativos.

Tabla 2 Tipos de sistemas operativos.

Sistemas operativos	Concepto
Multiusuario	Permiten que muchos usuarios utilicen sus programas al mismo tiempo, centenares hasta millares de usuarios.
Multiprocesador	Abrir un programa determinado en muchas computadoras.
Multitarea	Permite que en una misma computadora se puedan abrir varios programas.
Multitramo	Partes de un programa puedan ser procesados en forma simultánea.
Tiempo real	Respuesta inmediata a las funciones asociadas, los sistemas DOS y UNIX no poseen esta capacidad.

Fuente: Elaboración propia, según *www.olimpogeek.com*

2.1.8 Puertos

Un puerto es una ranura que se encuentra en la computadora y que permiten el acceso de los datos a través de una línea física, el que a su vez puede estar conectado a un router. Estos puertos están numerados, por ejemplo, el puerto 80 está asignado para las direcciones IP de internet.

Es una puerta de entrada muy buscada por quienes buscan vulnerabilidades en las computadoras

2.1.9 Sistema de supervisión y de acceso de datos

El control de supervisión y de acceso de datos, normalmente conocido como sistemas SCADA, son dispositivos físicos que controlan el funcionamiento de sistemas eléctricos, gasoductos, plantas potabilizadoras, etcétera en forma local o remota. Cuando hay un ciberataque a los sistemas SCADA, el ataque proveniente del plano virtual se transforma en un daño en el plano físico.

Estos sistemas poseen la características de ser robustos, ya que son instalados en diferentes infraestructuras, por lo tanto deben soportar altas temperaturas, movimientos, etc.

2.1.10 Firewalls

Son dispositivos que se utilizan para permitir el acceso de cierto tipo de tráfico hacia nuestra red o bloquear otros. Se pueden programar para el ingreso - egreso de datos, desde el nivel de puerto y protocolo hasta el nivel aplicaciones. En la tabla siguiente se observan distintos tipos de firewalls.

Tabla 3 Tipos de Firewalls.

Firewall	Concepto
De red	Se utilizan para regular el tráfico teniendo en cuenta las direcciones IPs internas con la IPs externas de una red.
Personales	Son de uso personal, se utilizan para regular el tráfico de las computadoras y demás máquinas, generalmente vienen incorporados con programas antivirus.
Aplicación Web	Se encuentran en aplicaciones web y en el internet, se utilizan para evitar la infección de virus provenientes de páginas web.
De base de datos	Se utilizan para proteger las bases de datos.

Fuente: Elaboración propia, según Arquitectura de seguridad informática, páginas 46 y 47.

2.1.11 Aplicaciones en la nube

Son aplicaciones web que se encuentran en las páginas del proveedor del servicio de internet. Esta forma de almacenamiento evita los costos de tener sólidas infraestructuras y, de alguna forma, transferir la responsabilidad de la seguridad informática de los datos a una empresa a cargo de terceros. Aquí cobra vital importancia la confianza en la empresa que resguarda los datos y el prestigio que tiene la misma en el mercado.

2.1.12 Honeypots

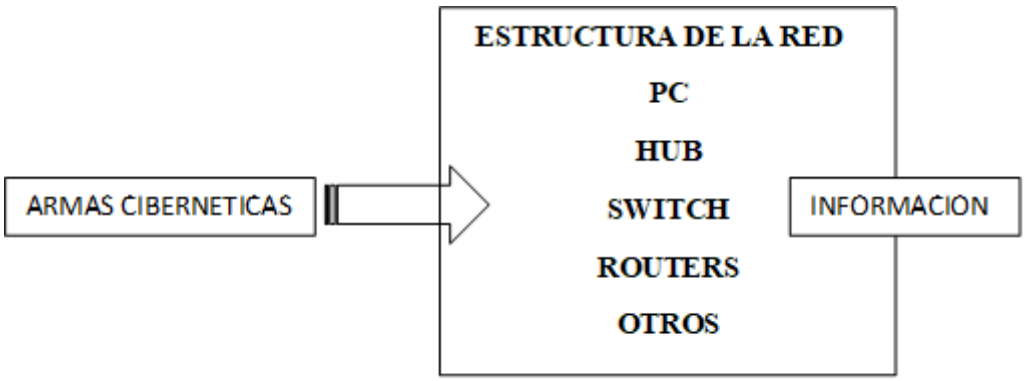
Son dispositivos que se utilizan para brindar seguridad a la arquitectura de red. El honeypots tiene la capacidad de reproducir IPs virtuales, de manera tal que cuando un intruso inicia con su ataque, este dispositivo emite una alarma.

Este dispositivo puede emular varias máquinas, por lo tanto el intruso no sabrá, en un primer momento si es una computadora real o no, dando tiempo al defensor para detectar la intrusión.

2.2 Armas cibernéticas

Seguidamente, se dan conceptos básicos sobre las armas cibernéticas que tienen por objetivo afectar los dispositivos recientemente señalados y que van a conformar la estructura de la red, en la intención de afectar la información que se almacena en ellas, como se observa en el esquema de la figura 3.

Figura 3 Esquema de ataque cibernético.



Fuente: elaboración propia.

Las armas cibernéticas serán utilizadas para afectar, a través de una vulnerabilidad en los sistemas del oponente, la confidencialidad, integridad y la disponibilidad de la información contenida en la estructura de la red o bien tratar de generar efectos, como la degradación o destrucción de infraestructuras críticas. Las más conocidas son las que se presentan en el siguiente cuadro y se considera de interés que el lector las conozca para poder entender el efecto que causan en los procesos informáticos.

2.2.1 Ataque de denegación de servicio distribuido

También conocido como ataque DDoS por sus siglas en inglés, consiste en generar un gran flujo de datos, que pueden partir desde varios lugares de conexión y que se los enfoca hacia el punto donde se quiere atacar. Esta acción imposibilita al usuario atacado operar, ya que su

computadora no puede procesar un volumen de información tan grande y el sistema se cae.

2.2.2 Troyanos

Son programas maliciosos que se encuentran dentro de otros programas que no lo son. Cuando el usuario, sin saberlo, abre un determinado programa infectado con un troyano, este se activa dentro de la computadora y puede afectarlo de distintas maneras.

Generalmente se utilizan para tomar el control de la computadora por parte del atacante, para borrar archivos, robar archivos, entre otros.

2.2.3 Ingeniería social

Se trata de todo un arte de engaño donde, con técnicas psicológicas o de manipulación, se trata de convencer a la persona atacada para que brinde la información que el intruso desee. Esta información puede incluir contraseñas, o cualquier otro tipo de dato que el atacante necesite para afectar la información de la víctima.

2.2.4 Exploits

Es programa diseñado para atacar una vulnerabilidad que tiene un sistema informático. Normalmente el que ataca utilizando esta técnica busca errores de programación, y una vez detectado esto, inyecta un código malicioso que se activa cuando se ejecuta el programa original, de allí su nombre de explotar una vulnerabilidad.

2.2.5 Crackers inalámbricos

Es un dispositivo que se utiliza para descubrir el passwords de las redes de wifi. Este dispositivo emite una señal de manera tal que desconecta a todos los usuarios que integran una red de wifi, al ejecutarse la reconexión por parte de los usuarios, esa señal es captada por el intruso y puede descifrar la clave para posteriores ataques.

2.2.6 Rootkits

Es un programa que se utiliza una vez que se tiene acceso como administrador de una red. Con el permiso de administrador, el atacante informático puede ejecutar otros programas maliciosos y al tener el control del sistema, se hace muy difícil su detección.

2.2.7 Inyectores

Son programas que se utilizan para ingresar códigos del tipo SQL o de Javascript a las aplicaciones web y así acceder a las bases de datos que se encuentran en esas páginas web.

Una vez dentro de las bases de datos, la información que allí se encuentra puede ser copiada, modificada, eliminada, etc.

2.2.8 Analizadores de tráfico

Es un programa espía que se instala en las computadoras y permiten analizar los datos que están circulando por esa red. A través de este software el atacante puede obtener información de su interés, como así también passwords de otros dispositivos y ampliar su ataque.

2.3 Otros conceptos importantes a tener en cuenta

2.3.1 Ciberespacio.

Se puede entender al ciberespacio como el lugar donde interactúa la información digital. Es un espacio virtual creado por el hombre y donde se hace necesario que exista una arquitectura de red que posibilite la transmisión, recepción y almacenamiento de datos.

Conocido como el quinto dominio del ambiente operacional, el ciberespacio tiene vital importancia para el planeamiento de las operaciones, ya que todos los componentes que lo conforman inciden en los conflictos de la actualidad.

2.3.2 Ciber amenaza

Son las acciones de carácter hostil que lleva adelante un actor cualquiera, militar o no, y que afectan a una arquitectura de red o infraestructura crítica con el objetivo de producir algún efecto que le proporcione al atacante una ventaja.

2.3.3 Ciber atribución

Consiste en detectar, localizar e identificar al actor o el lugar de donde proviene un ciberataque. Es de por sí una actividad sumamente difícil de lograr; requiere de la cooperación de actividades de ciber inteligencia.

2.3.4 Ciber disuasión

Consiste en lograr un efecto sobre un atacante, de manera tal, que desista efectuar su acción hostil al evaluar las condiciones de costo-beneficio.

2.3.5 Propiedades de la información

Es un concepto que cobra particular importancia debido a que si se logra afectar a la información, seguramente se afectará en gran medida a la organización. Por lo tanto, se

deberá proteger, en el ámbito del ciberespacio la confidencialidad, la integridad y la disponibilidad de la información (CID).

2.3.5.1 Confidencialidad

Está relacionada con la necesidad de saber, por lo tanto, es una propiedad que consiste en que la información esté accesible, en oportunidad, a la persona indicada.

2.3.5.2 Integridad

Propiedad que consiste en que la información no sea alterada en su forma o su contenido, es decir que mantenga las características propias configuradas por el autor.

2.3.5.3 Disponibilidad

Tiene que ver con la confiabilidad en los sistemas para que la información pueda ser utilizada cuando se la requiera.

2.4 Relación entre los elementos del diseño operacional y la guerra cibernética

2.4. 1 Nivel operacional

Teniendo en cuenta las definiciones, conceptos y conclusiones del primer capítulo, donde se desarrollaron los elementos del diseño operacional, sumado a las relacionadas con la cibernética, ahora se establece una posible relación entre ellos desde el punto de vista de la estrategia operacional.

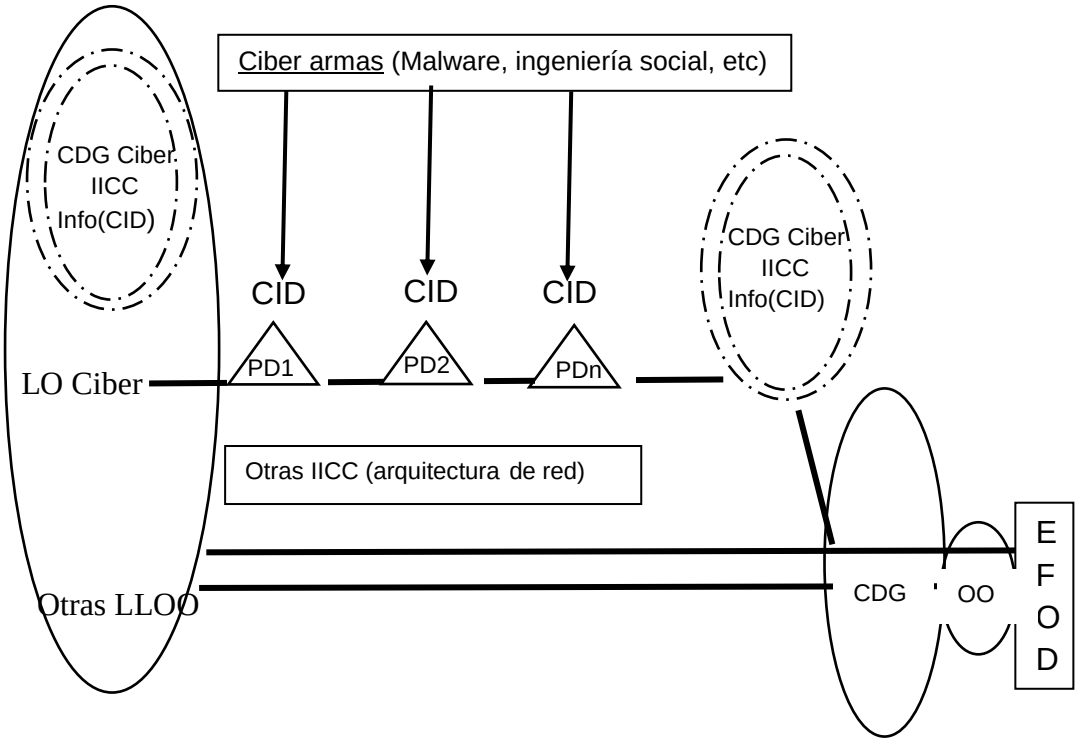
El centro de gravedad cibernético propio estará constituido por las infraestructuras críticas y la información contenida en ella, protegiendo sus propiedades (CID). De este centro de gravedad saldrá la línea de operaciones cibernética propia (LO Ciber) que tendrá el carácter de contribuyente, a los fines de colaborar con la consecución del centro de gravedad del oponente, como una línea de operaciones más, pero independiente y con un responsable a cargo de su conducción.

Esta línea de operaciones unirá los puntos decisivos que, en este nivel, podrán ser las infraestructuras críticas, que tendrán las características del objetivo operacional (decisivo, obtenible, definido). Esos puntos decisivos serán atacados a través de las armas cibernéticas, que buscarán las vulnerabilidades de la estructura de red del oponente, tratando de afectar las propiedades de la información (CID).

El centro de gravedad cibernético del oponente (infraestructura crítica esencial) estará protegido, al igual que el CDG propio, en forma de anillos buscando cambiar tiempo por espacio para equilibrar lo más rápido posible el sistema una vez atacado, la ciber resiliencia. En el grafico será representado con anillos discontinuos (frontera porosa) y concéntricos, dando la imagen correcta que adopta un CDG Cibernético.

Los aspectos de que se han hecho mención se representan en forma esquemática en la figura 4.

Figura 4 Elementos de diseño operacional en cibernéticos.



Fuente: elaboración propia.

Si las propiedades de la información (CID) son de vital importancia, entonces se pueden establecer las formas en que estas pueden ser afectadas, es decir que, para la confidencialidad, el efecto necesario para su vulneración será la *obtención* de la información. Para la integridad, será la *alteración* de la información y para la disponibilidad la *negación* de la información.

2.4.1.1 Obtención de la información

Consiste en vulnerar los sistemas defensivos del oponente e ingresar a sus datos, preferentemente almacenados dentro de su centro de gravedad cibernético y obtener la información de carácter confidencial.

2.4.1.2 Alteración de la información

Consiste en, una vez obtenida la información, modificarla, destruirla, encriptarla, o afectarla de cualquier otro modo, de manera tal que esos datos no sean iguales a las generadas por su autor.

2.4.1.3 Negación de la información

Este efecto consiste en impedir el acceso a los datos que necesita el oponente, de esta forma la información, de carácter sensible, deja de estar disponible.

En la tabla 4 se observa un modelo de tabla de doble entrada, con un posible esquema de afectación de la información en las infraestructuras críticas, a modo de ejemplo:

Tabla 4. Matriz de nivel operacional.

INFRAESTRUCTURAS CRÍTICAS	**OBTENCION DE LA INFORMACION**	**ALTERACION DE LA INFORMACION**	**NEGACION DE LA INFORMACION**
Central Nuclear (**CDG** Cibernético)	Saber niveles temperatura. Analizar niveles de radiación.	Modificar ciclos de refrigeradores.	Bloquear servidores.
Otras IICC			
Distribución de Agua (PD 1)	Analizar los niveles potabilización.	Modificar parámetros de potabilización .	Saturar. DDoS.
Gasoducto (PD 2)	Analizar los niveles de presión.	Modificar parámetros.	Apagar pantallas.
Otros (PD n)			

Fuente: Elaboración propia.

Una vez que el nivel operacional ha obtenido la infraestructura crítica esencial, definirá los efectos necesarios que, luego, el nivel táctico deberá obtener a través de las ciberoperaciones.

El nivel táctico de la conducción además de lograr los efectos sobre las infraestructuras críticas que les impone el nivel operacional, deberá obtener y afectar el centro de gravedad cibernético de su propio nivel.

En el nivel táctico el centro de gravedad cibernético se determina en base a los componentes informáticos de sus sistemas de armas o de sus sistemas de comando y control.

Tabla 5. Centro de gravedad cibernético.

CDG Sistema misiles antiaéreo S-300.	**Capacidad Crítica** Derribar aviones en vuelo a largas distancias.
Vulnerabilidad Crítica Sistema de radares perturbado.	**Requerimiento Crítico** Sistema de radares de localización y adquisición de blancos.

Fuente: elaboración propia en base a las clases recibidas durante el Curso Nivel I ESGC.

2.4.2 Una forma de defender el centro de gravedad cibernético

Es importante anular las actividades correspondientes a la ingeniería social que va a emplear el oponente con la intención de detectar vulnerabilidades y encontrar objetivos de ataque. En este sentido volvemos al concepto de ciber-fricción, donde es necesario la adecuada instrucción y adiestramiento de los usuarios de sistemas informáticos para minimizar el alcance de la agresión.

Este adiestramiento incluye el análisis de seguridad sobre los sistemas propios, donde a través de reconocimientos pasivos, como ser el uso de motores de búsqueda, de reconocimiento activo como ser detectar puertos activos, lo que se pretende es encontrar las vulnerabilidades propias que pueden resultar en los objetivos de ataque del adversario.

Conscientes de que los sistemas son vulnerables, la arquitectura de red adoptada, contempla la necesidad de una defensa que genere el mínimo de espacio por el máximo de tiempo, como ser el empleo de firewall y honeypots.

Si la intrusión tiene éxito, es probable que el responsable pase a una fase de consolidación del ataque, en donde trata de pasar desapercibido dentro de la red y finalmente hace la explotación sobre las propiedades de la información.

Finalmente, la fase de borrar los rastros de la intrusión al sistema es la actividad que se desarrolla para que el ataque sea efectivo.

Estas son las ideas generales a observar para la defensa del centro de gravedad cibernético propio, ya que desde el punto de vista técnico existen diferentes técnicas o tipos de análisis de seguridad.

2.5. Conclusión parcial del segundo capítulo.

Por lo investigado, las acciones de ciberguerra tienen características particulares, porque el ambiente operacional donde se desarrolla es el ciberespacio. Si bien las acciones se desarrollan en este espacio virtual pueden tener consecuencias en el plano real.

Durante el planeamiento del nivel operacional, las ciberoperaciones pueden ser planificadas utilizando como herramienta los elementos del diseño operacional, adaptándolas a las particularidades que este dominio virtual implica.

El centro de gravedad cibernético se debe determinar tanto para el nivel operacional como para el nivel táctico. El primero sobre la infraestructura crítica esencial y el segundo sobre los sistemas de armas y los sistemas de comando y control.

Con la idea de que todos los sistemas son vulnerables, se diseña la arquitectura de red que posibilite una eficaz defensa del centro de gravedad cibernético propio. Sabiendo cómo defenderlo, se deduce la forma de atacar el centro de gravedad cibernético propio, para esto es necesario la adecuada instrucción y adiestramiento en ataque y defensa.

CONCLUSIONES

El quinto dominio tiene la particularidad de estar en constante avance tecnológico, esto sumado a las nuevas formas de hacer la guerra, permite que estos avances de aplicación para el bienestar de las personas sean tomados como armas de ataque en un espacio virtual.

En el ámbito estrictamente militar, en donde las maquinas toman cada vez mayor protagonismo, genera una necesidad de toma de decisiones más veloces ante un contexto muy complejo.

La presencia de actores no militares, como combatientes en este teatro de operaciones cibernético, complejiza aún más el escenario e influye al momento de elegir el objetivo operacional.

Por lo expresado y ante las conclusiones parciales de esta investigación, es necesario un adecuado método de planeamiento que facilite la toma de decisiones, detecte vulnerabilidades y plantee un eficaz modo de atacar al subsistema cibernético del oponente.

La hipótesis planteada en este trabajo final integrador indica que los elementos del diseño operacional son afectados en forma parcial por las operaciones de guerra cibernética y deben ser considerados de manera particular.

La opción planteada ofrece una adaptación a ciertos conceptos doctrinarios a la luz del efecto de la guerra cibernética en los elementos del diseño operacional, de tal modo el autor ha presentado un modelo, totalmente perfectible, pero que sirve a modo de guía a ser utilizado en el planeamiento.

En el diseño operacional que se plantee para alcanzar el centro de gravedad cibernético del enemigo, surge la necesidad de una línea de operaciones particular, llámese una línea de operaciones cibernética. Ésta deberá contar un responsable en materia de ciberdefensa que la conduzca para asesorar y asistir al comandante y afectar el centro de gravedad cibernético del oponente.

En el nivel operacional de la conducción el centro de gravedad cibernético comprenderá una infraestructura crítica esencial del oponente y también determina los efectos que asignará al nivel táctico y que éste debe alcanzar.

En el nivel táctico de la conducción podrá hacer uso de esta herramienta de planeamiento convenientemente adaptado para cumplir los efectos que le determine el nivel operacional y

para determinar el centro de gravedad cibernético táctico, orientado hacia un subsistema de armas o de comando y control.

El planeamiento del nivel operacional, particularmente los elementos del diseño operacional, tienen su origen cuando el ciberespacio aún no era tenido en cuenta como un ambiente para la ciberguerra.

En esta investigación se han desarrollado estos dos componentes, por un lado aspectos de planeamiento y por otro, un nuevo dominio. De esta interacción surge un producto que sugiere una adaptación de aquellos elementos del diseño operacional que el autor consideró relevantes para alcanzar el centro de gravedad informático enemigo.

Finalmente señalar que el objetivo primordial de los ataques cibernéticos estará dado sobre las propiedades de la información, la confidencialidad, la integridad y la disponibilidad. En base a este parámetro el centro de gravedad cibernético propio debe ser defendido, con la certeza que de una u otra forma es vulnerado.

De la misma certeza de vulnerabilidad respecto de un centro de gravedad cibernético, se utilizan los elementos del diseño operacional, adaptados a la necesidad de operar en un dominio que va a tener usuarios, infraestructuras, dispositivos, espacio electromagnético, programas, aplicaciones, entre otros, sobre los cuales se pensarán los elementos del diseño operacional para afectar la información del oponente.

BIBLIOGRAFÍA

Kenny, A., Locatelli, O., Zarza, L. (2015). *Arte y diseño operacional*. Ciudad Autónoma de Buenos Aires: Escuela Superior de Guerra Conjunta.

Centro de Excelencia de Ciberdefensa Cooperativa de la OTAN. (2013). *Manual Tallin.* Cambridge: Universidad de Cambridge.

Cisneros, E. H. (2012). *Desafíos operacionales en el ciberespacio como nuevo campo de lucha* (Trabajo Final Integrador). Escuela Superior de Guerra Conjunta de las Fuerzas Armadas. Obtenido dehttp://cefadigital.edu.ar/handle/123456789/249

Estado Mayor Conjunto de las Fuerzas Armadas. (2012). *PC 00-01 Doctrina Básica para la Acción Militar Conjunta.* Buenos Aires: EMCFFAA.

Estado Mayor Conjunto de las Fuerzas Armadas. (2017). *PC 20-01 Planeamiento para la Acción Militar Conjunta - Nivel Operacional - Proyecto.* Buenos Aires: EMCFFAA.

Estado Mayor Conjunto de las Fuerzas Armadas. (2018). *PC 00-02 Glosario de Términos para la Acción Militar Conjunta - Proyecto.* Buenos Aires: EMCFFAA.

Estado Mayor General del Ejército. (1998). *Organización y Funcionamiento de los Estados Mayores - Tomo I.* Buenos Aires: Instituto Geográfico Militar.

Estado Mayor General del Ejército. (2015). *ROB 00-01 Conducción de las Fuerzas Terrestres.* Buenos Aires: Instituto Geográfico Nacional.

Giudici, D. E. (2013). *Lineamientos para la seguridad cibernética en Teatro de Operaciones* (Trabajo Final Integrador). Escuela Superior de Guerra Conjunta de las Fuerzas Armadas. Obtenido de http://cefadigital.edu.ar/handle/123456789/176

Larronde, J. M. (2012).*Dificultades para la obtención de la sorpresa en el nivel operacional ante el avance de las nuevas tecnologías de la información*. (Trabajo Final Integrador). Escuela Superior de Guerra Conjunta de las Fuerzas Armadas. Obtenido de http://cefadigital.edu.ar/handle/123456789/283

Ministerio de Defensa. (31 de Julio de 2018). Directiva Política de Defensa Nacional. *Decreto 703/2018*. Buenos Aires, Ciudad Autónoma de Buenos Aires, Argentina: Boletín Oficial.

Páez, E. P. (2014). *La guerra cibernética en el nivel operacional* (Trabajo Final Integrador). Escuela Superior de Guerra Conjunta de las Fuerzas Armadas. Obtenido dehttp://cefadigital.edu.ar/handle/123456789/147

Programa Avanzado en Introducción a la Ciberdefensa y la Ciberseguridad. Buenos Aires. ESGC.

Reynoso, S.C. (2013). *Arquitectura de Seguridad Informática.* Impreso en USA.

Rivolta, A. S. (2012). *Las vulnerabilidades de las operaciones militares derivadas de las redes sociales en Internet.*(Trabajo Final Integrador). Escuela Superior de Guerra Conjunta de las Fuerzas Armadas. Obtenido de http://cefadigital.edu.ar/handle/123456789/275

Sallis, E., Caracciolo, C., Rodríguez, M. (2010). *Ethical Hacking. Un enfoque metodológico para profesionales.* Buenos Aires: Alfaomega.

Sepetich, S. E. (2016). *Las Ciberoperaciones aplicadas a un Teatro de Operaciones – estudio de caso: Guerra Ruso Georgiana* (Trabajo Final Integrador). Escuela Superior de Guerra Conjunta de las Fuerzas Armadas. Obtenido de http://cefadigital.edu.ar/handle/ 123456789/900

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

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

Trama, G.A. (2017). *Operaciones Cibernéticas: su naturaleza, propósito y conducción*. Buenos Aires: Visión Conjunta, año 9, Nº 17, 56-59. Obtenido de http://cefadigital.edu.ar/handle/123456789/924

Uzal, R (2012). *Guerra Cibernética. ¿Un Desafío para la Defensa Nacional?* Buenos Aires: Visión Conjunta, año 4, Nº 7.

Uzal, R (2015). et al *Ciber Lavado Transnacional de Activos* publicado, referato mediante, en los anales de las 44 Jornadas Argentinas de Informática e Investigación Operativa. SADIO. Obtenido de http://44jaiio.sadio.org.ar/sites/default/files/sie160-179.pdf

Uzal, R (2015). *El Problema de la Ciber Atribución.* Buenos Aires: Consejo Argentino para las Relaciones Internacionales. Obtenido de http://www.cari.org.ar/pdf/boletin61.pdf

Uzal, R (2015). *Ciber Ius Ad Bellum.* Aportes para definir las reglas de empeñamiento militar de Argentina y de otros países de la Región en los casos de Ciber-Conflictos entre estados naciones. Buenos Aires: Consejo Argentino para las Relaciones Internacionales. Obtenido de http://www.cari.org.ar/pdf/boletin62.pdf

Uzal, R (2016). *Ciberdefensa: El Factor Crítico de Éxito Esencial.* Buenos Aires: Consejo Argentino para las Relaciones Internacionales. Obtenido de http://www.cari.org.ar/pdf/boletin63.pdf

Uzal, R (2016). *Ciber Disuasión.* Un capítulo particularmente sensitivo de la Ciberdefensa. Buenos Aires: Consejo Argentino para las Relaciones Internacionales. Obtenido de http://www.cari.org.ar/pdf/boletin64.pdf

Uzal, R (2017). *Ciber Califato y Ciber Hezbollah: consideraciones y propuestas.* Buenos Aires: Consejo Argentino para las Relaciones Internacionales. Obtenido de http://www.cari.org.ar/pdf/boletin65.pdf

Vergara, E. y Trama, G. (2017). *Operaciones militares cibernéticas: Planeamiento y Ejecución en el Nivel Operacional*. Buenos Aires: Visión conjunta. Obtenido de http://cefadigital.edu.ar/handle/123456789/939