



UNIVERSIDAD DE LA DEFENSA NACIONAL

INSTITUTO DE INTELIGENCIA DE LAS FFAA

“Sarg My D. José Antonio ÁLVAREZ DE CONDARCO”

**ESPECIALIZACIÓN EN GESTIÓN DE INFORMACIÓN MILITAR
TERRESTRE**

TRABAJO FINAL INTEGRADOR

**“Participación de elementos de inteligencia en operaciones de
ciberdefensa en el nivel táctico”**

Autor: Teniente Primero Lourdes Sabrina CARABAJAL

Director: Coronel (R) Augusto CAYO

Diciembre 2020

“Las ideas expresadas sólo representan la postura personal del autor, por lo que son de su absoluta responsabilidad, no reflejando en consecuencia la opinión del Instituto de Inteligencia de las Fuerzas Armadas y de la Universidad de la Defensa Nacional.”

Proyecto de Investigación	3
Introducción	8
Esquema gráfico metodológico	10
Capítulo I: Ciberespacio: el nuevo ámbito de las operaciones militares	11
Conclusiones parciales	16
Capítulo II: La Inteligencia Militar y el Ciberespacio	17
Conclusiones parciales	27
Capítulo III: El Ciberespacio, el nivel táctico y la Compañía de Inteligencia	29
Conclusiones parciales	33
Conclusiones Finales	34
Bibliografía	36

ELECCIÓN DE LA LÍNEA DE INVESTIGACIÓN

El presente trabajo de investigación intentará determinar la importancia de contar dentro del nivel táctico con personal de Inteligencia organizado y capacitado para enfrentarse a los diferentes riesgos en el ciberespacio que en la actualidad ocurren.

Resulta de interés para la Institución ya que, si bien se dieron los primeros pasos dentro del estudio de este nuevo ambiente, es preciso ahondar más en él para poder brindar una respuesta eficiente y eficaz ante las amenazas que en éste se desarrollan.

PLANTEAMIENTO DEL PROBLEMA

El problema formulado se basa en la necesidad de contar con elementos de Inteligencia en el nivel táctico que estén en capacidad de brindar apoyo a las actividades de ciberdefensa, así como personal adiestrado y capacitado para actuar dentro del ciberespacio.

PREGUNTAS DE INVESTIGACIÓN

¿Es la Ca Icia de la Br el elemento adecuado para poder brindar ese apoyo?

¿Qué se puede hacer frente a la necesidad de prevención, reducción de riesgos, alerta temprana, descubrimiento de vulnerabilidades, detección de incidentes y respuestas eficaces para, al menos, mitigar los efectos inmediatos?

¿Es suficiente el personal militar adiestrado?

¿Será necesario contar con elementos de inteligencia que complementen el abordaje de estas actividades de manera similar a como operan en los otros ambientes operacionales? ¿está el personal de Inteligencia en capacidad de afrontar estos esfuerzos?

JUSTIFICACIÓN DE LA INVESTIGACIÓN

El rápido y continuo avance de la tecnología generó un nuevo ambiente particular de interés en el cual se desarrollan sistemas críticos y esenciales. En él se pueden producir importantes efectos que causan pérdidas aún mayores que en los conflictos tradicionales.

Es por ello que esta nueva concepción de guerra “no guerra” generó que EEUU, Europa, India, Rusia y China comenzaran a conceptualizar estratégicamente sobre este tema y generar acciones necesarias que permitieron la creación de tropas adiestradas y equipadas para desarrollar operaciones en este nuevo ambiente, para la prevención del uso seguro de medios informáticos y de comunicaciones, la seguridad física de las instalaciones y la protección de diferentes medios de soporte de la información; las amenazas en el ciberespacio nos hacen pensar que es importante poseer un plan estratégico que abarque este nuevo plano de conflicto.

Éste nos permitirá identificar y neutralizar dichas amenazas, como así también detectar propias vulnerabilidades para luego reforzarlas y/o modificarlas.

Es por ello que el 14 de mayo de 2014, nuestro país creó el Comando Conjunto de Ciberdefensa del EMCO, que tiene como misión ejercer la conducción de las Operaciones de Ciberdefensa en forma permanente a los efectos de garantizar las operaciones militares del Instrumento Militar de la Defensa Nacional en cumplimiento de su misión principal.

En el nivel estratégico contamos con un Comando Conjunto y el personal adiestrado para realizar dichas operaciones, ahora bien, en el nivel táctico ¿poseemos personal adiestrado y capacitado para efectuar estas operaciones?

OBJETIVOS

OBJETIVO GENERAL

El objetivo general de este trabajo consiste en determinar la necesidad de contar con elementos de Inteligencia organizados y capacitados para realizar acciones dentro del ciberespacio.

OBJETIVOS ESPECÍFICOS

1) Identificar el alcance de las ciberoperaciones como un nuevo ámbito de guerra, a través del cual inciden directamente en el ambiente operacional.

2) Determinar la necesidad de contar con elementos de Inteligencia que operen en el ciberespacio.

3) Determinar las capacidades necesarias que debe afrontar el nivel táctico para operar dentro del ciberespacio con elementos de Inteligencia.

ANTECEDENTES

Una ciudad completa sin poder utilizar cajeros automáticos, servicios de banco online, sistemas de edición de periódicos que no permitían subir los artículos para su impresión y empleados estatales que no podían comunicarse a través de correos electrónicos, fue el resultado del primer ciberataque conocido que tuvo lugar en Estonia el 27 de abril del 2007. Las direcciones IP detrás de este atentado eran rusas, así como sus instrucciones, sin embargo, no son pruebas concretas de que Rusia haya estado detrás de esta ciberagresión.

En 17 de junio de 2010, la compañía de seguridad bielorrusa VirusBlokAda descubrió un malware que tuvo un papel central en lo que se considera el ciberataque más sofisticado de la historia. Stuxnet, fue el gusano que logró ralentizar el proceso de enriquecimiento de uranio en Natanz, una

instalación nuclear iraní. Afectó equipos con Windows y fue capaz de reprogramar controladores dañando sistemas de monitorización y control de procesos (SCADA). Cinco años más tarde en Ucrania, el virus BlackEnergy generó el primer apagón histórico eléctrico.

Este troyano ingresó a través de un “click” en un documento adjunto que recibió por correo electrónico un empleado de la central eléctrica. Se instaló automáticamente en tantos ordenadores como pudo, espiando todos los movimientos de la central. En un momento determinado, se instaló a distancia un módulo denominado KillDisk, programado para destruir archivos vitales de las computadoras de una central eléctrica. A continuación, provocaron el masivo apagón y activaron KillDisk para destruir las huellas de los hackers dentro del sistema.

Este nuevo escenario de conflicto es el que nos muestra un plano diferente para la guerra, en el cual el ciberespacio da lugar a acciones que afectan directamente la infraestructura crítica.

HIPÓTESIS DE INVESTIGACIÓN

La existencia de un nuevo ambiente específico para el desarrollo de las operaciones conlleva la necesidad de conformar elementos de Inteligencia organizados, equipados e instruidos para operar dentro de dicho ámbito.

ESTRATEGIA METODOLÓGICA

El presente trabajo se iniciará con un análisis de carácter general, para luego finalizar con conceptos específicos sobre el tema propuesto. Para ello, se recurre a distintas fuentes que permiten sustentar el desarrollo de la investigación mediante información referida al ciberespacio y las operaciones que allí se presentan. Asimismo, se hará referencia a hechos acontecidos de manera creciente en el mundo, donde se aprecia la explotación de esta nueva dimensión de guerra y

documentos públicos de países con cierto grado de desarrollo en el ámbito de interés, para establecer conclusiones parciales en cada capítulo, que sirvan de sustento a los fundamentos de la propuesta del presente TFI.

Se utilizará método exploratorio, buscando analizar los objetivos específicos que fueron establecidos, a través del análisis bibliográfico y documental.

Introducción

Un desconocido frente de conflicto, nuevos conceptos operacionales y misiones asociadas directamente con el uso de la tecnología de la información, son los puntos a considerar en la actualidad para “combatir” en este espacio.

El ciberespacio nos obliga a entender su composición y funcionamiento para enfrentar la integración de todos sus elementos y poder ejercer la seguridad y defensa mediante él. Son los conocidos ataques en Irán y Ucrania los que dieron lugar a un salto de dimensión como escenario de conflicto.

Hoy en día todo es Internet, vivimos en un mundo interconectado a la red. Si bien pasaron varios años desde estos eventos, no todos los países supieron adquirir la capacidad de afrontar esta evolución continua y permanente.

En nuestro país el 14 de mayo de 2014, se creó el Comando Conjunto de Ciberdefensa del EMCO, que tiene como misión ejercer la conducción de las Operaciones de Ciberdefensa en forma permanente a los efectos de garantizar las operaciones militares del Instrumento Militar de la Defensa Nacional en cumplimiento de su misión principal.

En el nivel estratégico contamos con un Comando Conjunto y el personal adiestrado para realizar dichas operaciones, ahora bien, en el nivel táctico ¿poseemos personal adiestrado y capacitado para efectuar estas operaciones?

El presente trabajo de investigación intentará determinar la importancia de contar dentro del nivel táctico con personal de Inteligencia organizado y capacitado para enfrentarse a los diferentes riesgos en el ciberespacio que en la actualidad ocurren.

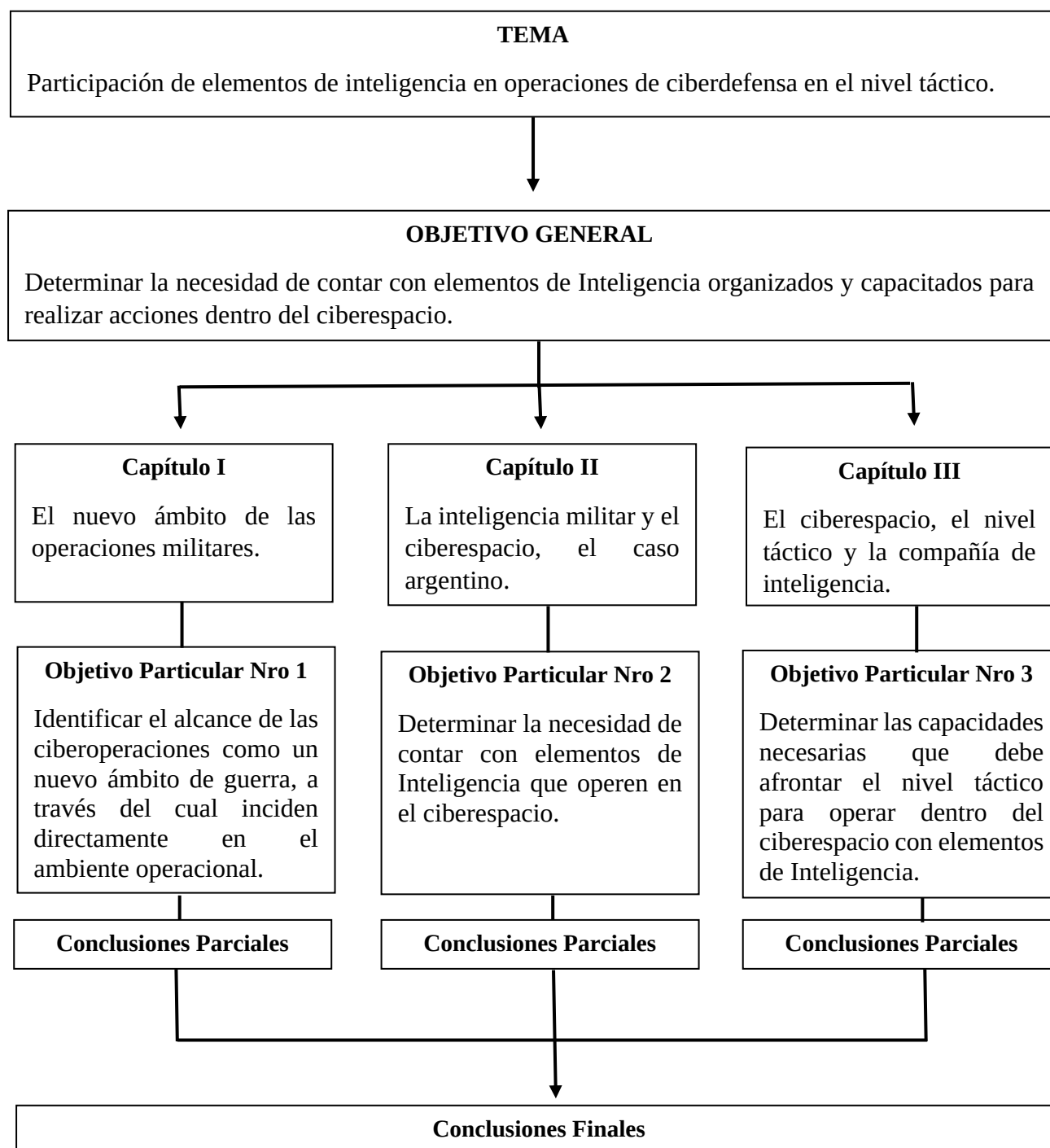
Resulta de interés para la Institución ya que, si bien se dieron los primeros pasos dentro del estudio de este nuevo ambiente, es preciso ahondar más en él para poder brindar una respuesta eficiente y eficaz ante las amenazas que en éste se desarrollan.

Es por ello que el presente trabajo se iniciará con un análisis de carácter general, para luego finalizar con conceptos específicos sobre el tema propuesto. Para ello, se recurre a distintas fuentes que permiten sustentar el desarrollo de la investigación mediante información referida al ciberespacio y las operaciones que allí se presentan. Asimismo, el desarrollo se estructurará en tres capítulos que respondan nuestro objetivo general de investigación y que aborden el objetivo específico propuesto para cada uno de ellos:

1. El capítulo I (“El nuevo ámbito de las operaciones militares”) responde al interrogante principal ¿Qué es el ciberespacio? En él se podrá entender la aparición de esta nueva dimensión, los tipos de acciones que se desarrollan y porque es importante para el ámbito militar.
2. El Capítulo II (“La inteligencia militar y el ciberespacio, el caso argentino”) determina el lugar en donde se encuentra nuestro país para afrontar estas nuevas acciones dentro de los documentos establecidos por la Inteligencia Nacional.
3. El Capítulo III (“El ciberespacio, el nivel táctico y la compañía de inteligencia”) aborda la importancia de la necesidad de contar con personal adiestrado y capacitado, a nivel GUC, para participar de las operaciones dentro del ciberespacio.

Para analizar el problema de investigación se utilizará método exploratorio, buscando analizar los objetivos específicos que fueron establecidos, a través del análisis bibliográfico y documental.

Esquema gráfico metodológico



CAPÍTULO I: CIBERESPACIO: EL NUEVO ÁMBITO DE LAS OPERACIONES MILITARES

La Real Academia Española, define al ciberespacio, como “ámbito artificial creado por medios informáticos”. (Real Academia Española, s.f.).

El ciberespacio es un escenario táctico, estratégico y operativo diferente de los espacios terrestre, marítimo, aéreo y espacial, su esencia está en el modo en que altera las realidades de los otros dominios (Carrillo, 2015).

Hoy, casi todas las actividades que realiza el hombre se desarrollan en el ciberespacio. Éste no permite el ejercicio del poder físico, no se controla la realidad y el individuo tiene la posibilidad de cambiarla. La diferencia con las guerras clásicas incide en el daño que puede causar, siendo muy superiores en la relación de costos – beneficios.

Otro punto importante es el hecho de que el causante posee ínfimas posibilidades de ser detectado. La localización de las acciones depende de la existencia de dispositivos tecnológicos y de la voluntad del operador para determinar el origen (así como las intenciones reales). Sin embargo, esto no asegura el éxito del descubrimiento del autor.

Cuando hablamos de ciberespacio hacemos referencia a un escenario en el cual no podemos definir sus límites, ya que trasciende los límites geográficos (sobrepasa el cómo y el cuándo), y tampoco detectar las operaciones que dentro de él se ejecutan. Ya sea una o varias personas sentadas a través de su computadora al mismo tiempo, el anonimato dentro de este ambiente brinda una extensión del tiempo que permite pensar y dar una respuesta.

Dado los ambientes operacionales en los que se desenvuelven las fuerzas militares, el conocimiento acabado de cada uno de ellos permite la flexibilidad para tomar decisiones teniendo en

cuenta en qué punto comienza y termina su espacio de responsabilidad. El ciberespacio genera una inmensidad de lugares que abarcan los ambientes ya conocidos, situados en la mente de las personas donde se desenvuelve todo. Esta nueva complejidad operacional aplica una importancia diferente a las anteriores.

Así como es casi imposible detectar su origen y autor, es no menos importante entender que aún cuando las acciones son intangibles, los resultados de cada uno de ellos no lo son. Si bien sus efectos pueden ser medidos, estudiados y determinados (con exactitud en muchos casos), el ritmo de batalla se genera en un ambiente completamente tecnificado que puede generar grandes pérdidas.

En la Argentina, el Libro Blanco de la Defensa, (Ministerio de Defensa, 2010) define al ciberespacio como: Las tecnologías destinadas a asegurar la confidencialidad, integridad y disponibilidad de la información esencial para mantener la continuidad operativa del ciberespacio que configura una nueva dimensión operacional –independiente y omnipresente– en los espacios terrestres, marítimos y aeroespaciales de jurisdicción e interés. Desarrollo de ingenios militares, capacidades, organizaciones y recursos humanos que aseguren el uso y el control del ciberespacio específico de los componentes del Sistemas de Defensa Nacional, y aquellos ámbitos de interés estratégico asociados ante agresiones externas contra el ciberespacio nacional. (p278).

En el año 2014 la Directiva Política de Defensa Nacional (DPDN) definió al ciberespacio como un ámbito transversal a los escenarios tradicionales del conflicto (mar, tierra, aire y espacio exterior), siendo la primera vez que Argentina definía conceptualmente al ciberespacio desde la óptica de la Defensa Nacional. Dicha conceptualización sería modificada en la siguiente DPDN del año 2018, la cual se refiere al ciberespacio como un quinto dominio de guerra.

De acuerdo con los conocimientos incorporados y planteados hasta este momento, se puede establecer que la necesidad primordial del comandante será lograr un mayor control del ciberespacio para determinar un ámbito de mayor seguridad, valga la redundancia, a las operaciones militares propias.

Ya sabemos, que en él se desarrollan actividades de creación, procesamiento, intercambio y visualización de datos e información digital, mediante redes, software, hardware y firmware de dispositivos electrónicos, cuyo carácter está establecido por el empleo de la tecnología. Ahora bien, planteando este campo de combate moderno, ante un ataque en el ciberespacio todo quedaría fuera de servicio, las redes de computadoras, la telefonía celular y los sistemas de control de tráfico (terrestre, aéreo y naval). Las autoridades gubernamentales estarían imposibilitadas de evaluar daños y de comunicarse con el mundo para informar la situación y poder proteger la vulnerabilidad de sus ciudadanos. Esta situación crítica impediría una toma de decisiones eficientes y rápidas.

El instrumento de poder militar, para poder ejercer su fuerza sobre los escenarios, requerirá disponer de unas capacidades militares defensivas y ofensivas y unos medios que permitan alcanzar la superioridad en cada entorno militar específico.

El reglamento de Conducción de las Fuerzas Terrestres, ROB-001, define al ambiente operacional como al “conjunto de factores de diversa naturaleza que existen de forma estable y semiestable en una determinada región”; y agrega que “ellos influirán en la determinación, de la composición, magnitud, equipamiento, aptitud de las Fuerzas que en él deban intervenir, como así también en la aplicación de su poder de combate”. Además de ocasionar un marcado efecto sobre la aplicación práctica de los conceptos doctrinarios podrá imponer ciertas limitaciones a la conducción

de las fuerzas terrestres (cualquiera sea su nivel), las cuales incidirán esencialmente sobre la libertad de acción”.

Menciona también, que durante el planeamiento se deberá tener en cuenta que el enemigo conocerá las vulnerabilidades de las vías de comunicación que se emplearán, adoptará seguramente medidas para evitar o reducir cualquier acción de interdicción propia. En tal sentido, el valor de la interdicción electrónica/cibernética, aumentará en tanto contribuya mediante la afectación de su comando y control, al limitar la capacidad de reacción del enemigo. Por otra parte, la ejecución de operaciones de velo y engaño como complemento de esta operación, aumentará la probabilidad de que su ejecución sea exitosa. Se deberá tener en cuenta que en toda operación táctica será necesario un apoyo de defensa cibernética que contribuya a garantizar la libertad de acción en las operaciones militares y proporcionen un adecuado nivel de seguridad en el empleo de los sistemas propios.

Por otro lado, uno de los grandes desafíos del ciberespacio está siendo la definición de los conceptos que han aparecido en este ámbito. Se habla con frecuencia indistintamente de ciberataque (a todos los niveles, sin tener en cuenta si ha sido un simple robo de una contraseña o un ataque a una infraestructura crítica) y de ciberguerra o ciberconflicto.

Si nos referimos a ciberataque, hacemos referencia a un conjunto de acciones ofensivas contra sistemas de información como bases de datos, redes computacionales, etc. hechas para dañar, alterar o destruir instituciones, personas o empresas. Puede dirigirse tanto a los equipos y sistemas que operan en la red anulando los servicios que prestan, como a los datos e información que se almacenan en bases de datos, robándolos o usándolos para espionaje. A su vez, podemos distinguir cuatro grupos importantes de ciberataque:

- Ciberdelincuencia: utilizando técnicas como el phishing, roban la identidad de personas o empresas para realizar fraudes bancarios, vaciar cuentas, etc, todo ello generalmente con fines económicos.
- Hacktivismo: en otras ocasiones, lo que ocurre es que los hackers vulneran páginas de empresas grandes o del gobierno, a veces, incluso desde tu propio ordenador, para realizar una protesta. El objetivo de estos ciberataques es ideológico, social, y dentro de los hacktivistas, la organización Anonymous es la más conocida.
- Ciberespionaje: compromete la ciberseguridad en las empresas, ya que trata del robo de información sensible y valiosa, como información financiera, de clientes, empleados... que además posteriormente puede venderse a muy altos precios en el mercado negro.
- Ciberterrorismo: suele ir dirigido contra gobiernos o países, afectando a servicios como salud o defensa, infraestructuras de gran importancia.

Cuando hablamos de ciberguerra, como definición general será la acción de un Estado – Nación para penetrar en las computadoras y las redes de otra nación con fines de causar daño o interrupciones a través, por ejemplo, de virus informáticos o ataques de denegación de servicio; algunos autores afirman que la guerra cibernética complementa la guerra tradicional y al mismo tiempo refleja sus usos y costumbres. En ella también hay soldados y espías: empleados de las fuerzas armadas y los servicios de inteligencia (muchos de ellos reclutados en universidades, pero también en el submundo de hackers delincuentes, dedicados a ejecutar misiones contra intereses de otros países).

Para cualquiera de estas acciones que hacen referencia cada uno de sus respectivos términos, será necesario incorporar medidas de carácter activo que permitan lograr la iniciativa. El marco

doctrinario actual no responde a las necesidades que impone la naturaleza de las actividades en el ciberespacio como una nueva dimensión de la guerra. La aparición de una dimensión con características particulares propias, que no responde a reglas obsoletas, plantea una larga lista de interrogantes al momento de enfrentar estas nuevas amenazas de forma integral y eficiente.

Conclusiones parciales

El ciberespacio es un ámbito con un diseño particular creado por el hombre. Nos presenta una diferencia fundamental con los espacios ya conocidos (terrestres, aéreos, marítimos) al no poseer límites tangibles y determinados. Es por ello que, entender su dominio por parte de nuestro país o de cualquier otro en el mundo, será un trabajo complejo y de evolución constante. No solo hablamos del control de este espacio, si no, también de la protección de cualquier ciberataque.

Teniendo en cuenta el anonimato de sus actores, sus intereses y objetivos, es difícil lograr una planificación, ejecución y desarrollo de capacidades acordes para anticipar y/o neutralizar amenazas que puedan afectar la infraestructura crítica del instrumento militar. Sin embargo, resulta necesario la adopción de un conjunto de medidas destinadas a prevenir la sorpresa, preservar la libertad de acción y negar al enemigo información sobre las propias fuerzas con la finalidad de proteger y preservar todos aquellos medios, infraestructuras críticas e información, contenidas en el ciberespacio.

CAPÍTULO II: LA INTELIGENCIA MILITAR Y EL CIBERESPACIO, EL CASO ARGENTINO

Para dar respuesta al segundo objetivo específico a tratar en el desarrollo de este trabajo, “determinar la necesidad de contar con elementos de Inteligencia que operen en el ciberespacio”, este segundo capítulo tendrá como eje investigar la presencia y la necesidad de la Inteligencia Militar en dicho ambiente, analizando el caso argentino.

Para poder analizar la injerencia de la inteligencia en el ciberespacio es necesario hacer un análisis sobre la definición de inteligencia estratégica, sus funciones y finalidades. Marcelo de los Reyes (2018) explica que la actividad de inteligencia debe desarrollarse para la adecuada toma de decisiones que sirve para prevenir y resolver conflictos que pueden derivar en crisis.

De esta forma, los conocimientos proporcionados por la inteligencia tienen por objeto servir de insumo para la toma de decisiones y, al hacerlo, la inteligencia adquiere valor en sí misma.

Cuando hacemos referencia a la inteligencia estratégica nos encontramos frente a una actividad proactiva, producida en el marco de una visión de futuro, de lo posible y deseable que produce conocimiento vital para la supervivencia nacional. Esta inteligencia se orienta a objetivos nacionales, ayudando a definir objetivos factibles, generando una base para el planeamiento y el logro de dichos objetivos. (Anónimo: 2009).

Sherman Kent (2016, p. 4) presenta a la inteligencia como conocimiento y advierte que “the intelligence activity consists basically of two operations. [...] Surveillance operation [...] and research operation”¹. La primera se refiere a “many ways by which the contemporary world is put under close and systematic observation”², mientras que la última equivale al “attempts to establish meaning

¹ Sherman Kent (2016, p. 4) La actividad de inteligencia consiste básicamente en 2 operaciones: operaciones de vigilancia y operaciones de investigación. (Trad. Princeton University Press).

² Sherman Kent (2016, p. 4) Formas a través de las cuales el mundo actual es puesto bajo observación. (Trad. Princeton University Press).

patterns out of what appears to be going on now”³. De esta forma, el conocimiento equivale entonces a una ventaja relativa por sobre la otra parte.

Se puede apreciar entonces que el conocimiento representa una ventaja a la hora de tomar decisiones sólo si este conocimiento es completo, seguro, entregado a tiempo y capaz de servir como base para la acción (Kent: 2016). Un conocimiento que cumpla con estos lineamientos sirve a la toma de decisiones de forma eficaz, obstaculizando y previniendo un cisne negro.⁴

Si traspoláramos las acciones descriptas por Kent al ciberespacio, la ciberinteligencia es la realización de operaciones de investigación y vigilancia en el ambiente cibernético.

Con cada avance tecnológico, mayor es la presencia de sistemas en el ciberespacio. Por lo cual aumenta la necesidad de contar con elementos de inteligencia, que a su vez lleva a diversos autores a intentar definir el rol del sistema de inteligencia en el ciberespacio, ya que no se discute la necesidad de contar con un sistema en dicho ambiente.

El coronel Matthew M. Hurley (2014) conceptualiza las tareas de inteligencia, vigilancia y reconocimiento (IVR) cibernético para contribuir a la doctrina de la Fuerza Aérea. Establece que a estas tareas las componen dos actividades: una “desde” y otra “para” el ciberespacio.

El coronel Hurley describe a la actividad “desde”, como la explotación de redes para emplear la información obtenida en apoyo de operaciones: es decir la obtención de datos de las redes del enemigo en busca de información con valor de inteligencia que se pueda recopilar en el ámbito cibernético a través de medios de comunicación, chats privados, videos, etc.

³ Sherman Kent (2016, p. 4) Intenta establecer patrones de significado de lo que arecer estar bien. (Trad. Princeton University Press).

⁴ Un cisne negro es un suceso considerado improbable, que cuando sucede tiene efectos devastadores. Para ampliar, ver Taleb, N. N. (2016). El Cisne Negro. El impacto de lo altamente improbable. Buenos Aires, España: Paidós

La segunda actividad “para”, es descripta como IVR para procurar la superioridad ciberespacial: es decir, alcanzar la necesidad de una capacidad de trabajo coordinado garantizando la producción de inteligencia y su posterior diseminación que permita desarrollar las operaciones cibernéticas con un estado de superioridad por sobre la del enemigo.

Por su parte Lourdes Puente Olivera existen dos formas o tipos de inteligencia. Una de ellas referida a la utilización del ciberespacio como medio para obtener información, mientras que la otra se vincula al ciberespacio en sí mismo, enfocado en el cómo operar dentro del dominio.

La autora trata de explicar que la inteligencia, específica de este ambiente, debe definir qué tengo y que hay que saber para conocer este espacio, ya que así se conocerán las vulnerabilidades y oportunidades propias que facilitarán el proceso de toma de decisiones.⁵

Hugo Miguel, otro de los autores que analiza la problemática, propone como definición de ciberinteligencia la siguiente:

“Proceso de búsqueda, localización, registro, análisis y diseminación de la información inherente al ciberespacio y tiene por objeto parametrizar las amenazas en ese ambiente, para lo cual debe ante todo generar las preguntas que nos permitan elaborar el índice básico de información y determinar los factores fijos propios (reales o virtuales) que identifican nuestro teatro de operaciones cibernético. En este aspecto, es importante para trabajar en una infraestructura de datos espaciales que nos permita llevar el mundo abstracto de la red al concreto del posicionamiento geográfico de la infraestructura de comunicaciones e informática. [...] La inteligencia

⁵ Puente, M. L. (1 de abril de 2018). Guía para entender la nueva geopolítica del ciberespacio. Perfil. (Consultado el 5 de diciembre de 2018 en <https://www.perfil.com/noticias/elobservador/guia-paraentender-la-nueva-geopolitica-del-ciberespacio.phtml>)

en el ciberespacio conlleva el conocimiento de plataformas, sistemas operativos, redes de acceso, métodos de acceso múltiple, técnicas de validación de usuario, análisis de tráfico y perfilado de paquetes, factores que son necesarios para poder generar los elementos esenciales de información que permitan realizar las preguntas correctas para obtener la información que un comandante necesita para asegurar el uso y control de la red. Determinar de manera proactiva las capacidades, la psicología y las motivaciones de nuestros atacantes permitirá prevenir y anticipar ataques reales a las redes y a las actividades propias en el ciberespacio.”⁶

De todas estas definiciones, se puede apreciar, que la función principal de la actividad de inteligencia en el ciberespacio es descifrar, de las actividades desarrolladas virtualmente, las consecuencias que traerán aparejadas en el mundo físico y así poder apoyar los distintos tipos de operaciones (sean éstas tradicionales o cibernéticas).

Ya definida la actividad de inteligencia en el ciberespacio, es importante determinar cómo se desarrolla la misma en el caso específico de Argentina. Para ello se analizará la evolución del marco legal que da entidad a las actividades de inteligencia en dicho ambiente, buscando diferenciar los ámbitos de seguridad y defensa, las estructuras que se encuentran en las mismas y principalmente las actividades que, enmarcadas en la ley, se desarrollan.

El marco legal que legitima la actividad de inteligencia abarca no sólo las leyes específicas de inteligencia, sino que también es importante el análisis de aquellas del sistema de seguridad interior y de defensa nacional ya que establecen los límites a los diferentes órganos que conforman la Agencia Federal de Inteligencia y a su vez extrapolar dichos conceptos al ambiente del ciberespacio.

⁶ Miguel, H. (15 de marzo de 2018). Mitos y realidades de la ciberdefensa. Revista DEF (consultado el 6/12/2018 en <http://defonline.com.ar/mitos-y-realidades-de-la-ciberdefensa/>)

Las divisiones pueden apreciarse claramente en las definiciones que aporta la ley de Inteligencia Nacional, su modificatoria y el decreto 1311/2015 que establece la nueva Doctrina de Inteligencia Nacional.

La ley N° 27.126 (2015), establece en su artículo segundo que la inteligencia nacional es “la actividad consistente en la obtención, reunión, sistematización y análisis de la información específica referida a los hechos, riesgos y conflictos que afecten la Defensa Nacional y la seguridad interior de la Nación.” Mientras que la ley 25.520, en su artículo segundo, define como:

“Inteligencia Criminal a la parte de la Inteligencia referida a las actividades criminales específicas que, por su naturaleza, magnitud, consecuencias previsibles, peligrosidad o modalidades, afecten la libertad, la vida, el patrimonio de los habitantes, sus derechos y garantías y las instituciones del sistema representativo, republicano y federal que establece la Constitución Nacional. Inteligencia Estratégica Militar a la parte de la Inteligencia referida al conocimiento de las capacidades y debilidades del potencial militar de los países que interesen desde el punto de vista de la defensa nacional, así como el ambiente geográfico de las áreas estratégicas operacionales determinadas por el planeamiento estratégico militar. Sistema de Inteligencia Nacional al conjunto de relaciones funcionales de los organismos de inteligencia del Estado Nacional, dirigido por la Secretaría de Inteligencia a los efectos de contribuir a la toma de decisiones en materia de seguridad exterior e interior de la Nación.”

Del análisis del artículo 2 de dicha ley se aprecia lo específico que hace a cada área de interés y sin dar lugar a libres interpretaciones, las principales diferencias entre seguridad interior y defensa

nacional haciendo eco de las cuestiones de inteligencia cuando establece un sistema de inteligencia nacional dividido en tres agencias con responsabilidades propias y limitadas.

Es decir que el sistema de seguridad interior es el encargado de desarrollar la inteligencia referida a cuestiones criminales, mientras que, el sistema de defensa nacional se encargará únicamente de producir inteligencia en cuestiones referidas a la defensa nacional y al instrumento militar. Es importante destacar, entonces, que por ley estas agencias deben mantenerse separadas sin inmiscuirse en las tareas otorgadas a la otra.

Al comparar dichos conceptos con las principales potencias mundiales o con los países de la región se destaca la naturaleza propia de un sistema que divide la seguridad interior de la defensa nacional incrementando las dificultades que ofrece el ciberespacio para desmembrar qué corresponde a seguridad interior y qué forma parte de la defensa nacional.

En lo que atañe el hecho de que la Inteligencia Estratégica Militar no está habilitada para tratar cuestiones vinculadas a la ciberseguridad y a la seguridad de la información, que nos permite concluir que solamente las cuestiones vinculadas al sistema de defensa nacional en el ciberespacio serán objeto de consideración por parte de la última agencia en cuestión.

Dicha norma legal establece como los principales destinatarios a:

- 1) El Presidente de la Nación
- 2) Los Ministerios de Defensa y Seguridad
- 3) Otros ministerios.

Es así entonces, que los insumos aportados por la inteligencia nacional deben nutrir las políticas de defensa nacional y seguridad interior en base a problemáticas relevantes.

Es importante destacar que la ley distingue que la Dirección Nacional de Inteligencia Criminal (DINICRI), es responsable de la producción de inteligencia criminal, mientras que los referidos a delitos criminales complejos, contra poderes públicos y el orden constitucional dependerán de la Agencia Federal de Inteligencia (AFI).

A su vez la Dirección Nacional de Inteligencia Estratégica Militar (DINIEM), es responsable de la producción de inteligencia estratégica militar, dejando la producción de inteligencia operacional y táctica, en manos de los organismos de inteligencia dependientes de las Fuerzas Armadas (Comando Conjunto de Ciberdefensa y Direcciones de Ciberdefensa específicas de cada Fuerza).

Ya establecidos los ámbitos en que divide la ley la aplicación de los servicios de inteligencia (seguridad interior y defensa nacional) y a su vez los organismos que dan respuesta a cada ámbito, junto a las principales responsabilidades que deben cumplir cada una de ellas (DINICRI, AFI, DINIEM), es necesario analizar cómo se realizan las diferentes actividades dentro del sistema de inteligencia nacional.

Al referirnos a la inteligencia como actividad, se aprecia que el proceso de investigación puede iniciarse de dos formas: por requerimiento político, al recurrirse a ella en busca de datos o antecedentes, o cuando el sistema de inteligencia inicia una investigación por propia observación de lo que ocurre en el contexto. (Kent: 2016).

Es importante analizar los diferentes derroteros que siguieron los organismos del sistema de inteligencia en Argentina al iniciar el proceso de investigación de cuestiones cibernéticas (de ambas formas explicadas anteriormente), comprendiendo su deber de analizar la temática.

El fenómeno del ciberespacio como nuevo ambiente operacional y el empleo de elementos de inteligencia en el mismo, inició en la DINIEM antes que en la DINICRI. Sin contar que dicha temática

ya era analizada desde hacía varios años por las dependencias de inteligencia de cada fuerza (armadas y de seguridad).

Por ejemplo, en el Ministerio de Defensa (MINDEF), el Proyecto de Capacidades Militares (PROCAMIL) de 2010, elaborado en el marco del Estado Mayor Conjunto (EMCO), incluía las cuestiones de ciberdefensa como capacidades de inteligencia, que fue tomado con mayor detalle en el siguiente documento de planeamiento del MINDEF (PLANCAMIL de 2011), que incorporaba la ciberdefensa en el Área de Capacidad 3 (AC3) “Vigilancia, Reconocimiento e Inteligencia”. (Albarracín y Eissa: 2019).

Simultáneamente al desarrollo de los documentos anteriormente mencionados, la cuestión cibernética fue un tema analizado por la DINIEM en 2011 que, sin un requerimiento político formal, respondiendo directamente a la observación sobre el contexto internacional, y en cumplimiento de la función que emana de los organismos de inteligencia de anticipar, se dedicó al análisis de éste.

Durante dicho análisis el principal interrogante que se planteaba versaba sobre el rol y la responsabilidad de la inteligencia en materia cibernética, para lo cual, el Ministerio de Defensa requirió a la DINIEM un estudio con el objeto de identificar las capacidades cibernéticas adquiridas con la finalidad de coordinar esfuerzos.

Durante el año 2012, la DINIEM organizó un debate del que participaron representantes de las Fuerzas Armadas y que tenía por objeto la definición conceptual de ciberdefensa. El eje del debate fue el análisis conceptual, ya que dependiendo de la definición a la que arribara se apreciarían las responsabilidad y funciones del sistema de defensa nacional en el ciberespacio.

El documento alcanzado se elevó al Ministerio de Defensa en octubre de ese mismo año, pero la Dirección General de Planeamiento y Estrategia (DGPLA) no estuvo de acuerdo con los resultados, por lo que el documento no logró obtener resultado alguno. (Albarracín y Eissa: 2019).

Durante el año 2013, el MINDEF sufrió un ataque cibernético que vulneró la seguridad de información confidencial.

Este hecho difundió proyectos de investigación y desarrollo, el estado real de las FFAA y de los sistemas de armas, información personal de los trabajadores del MINDEF y el área en el que cada uno desempeñaba sus funciones.

Estos hechos impulsaron al Ministerio de Defensa a que empezara a considerar los riesgos inherentes de confundir operacionalmente los términos ciberinteligencia y ciberdefensa, forzando la necesidad de diferenciar medidas de seguridad de la información de las de ciberinteligencia, dilatando aún más el accionar de la DINIEM. (Albarracín y Eissa: 2019).

Es a partir del año 2013 que se estudia en profundidad la incumbencia del sistema de inteligencia argentino en el ciberespacio, cuando desde Jefatura de Gabinete de Ministros se refieren a los logros del Sistema de Inteligencia Nacional (en concordancia con el Plan de Inteligencia Nacional vigente) y detallan que la producción de inteligencia en materia de defensa nacional y seguridad interior involucró el profundo análisis de las ciberamenazas. (Jefatura de Gabinete de Ministros: 2014).

Con la sanción de la ley N° 27.126 y el Decreto N° 1311 (ambos de 2015), se inicia la producción de inteligencia referida a la ciberseguridad y la ciberdefensa, en concordancia con el Plan de Inteligencia Nacional vigente.

Es así que se establecieron los límites de escenarios definidos de acuerdo a las diferentes prioridades de los asuntos estratégicos enmarcados en dicho plan.

El Decreto 1311/2015 estableció la creación de la Dirección Operacional de Inteligencia sobre Ciberseguridad (DOC) dentro de la AFI. La cual empezó a trabajar en noviembre de 2015⁷ con la misión de producir “inteligencia orientada al conocimiento de las acciones que atenten contra la ciberseguridad en el marco de la defensa nacional y la seguridad interior, y de los grupos nacionales o extranjeros responsables de llevarlas a cabo” (Anexo 2, folio 66).

La producción de inteligencia nacional sobre seguridad interior se limitó al abordaje de temáticas como: “Narcotráfico, Trata de Personas, Tráfico de Armas, Delitos Económicos y Financieros, Terrorismo y Atentados contra el Orden Constitucional, Ciberseguridad y Contrainteligencia Institucional y Criminal.” (Jefatura de Gabinete de Ministros: 2016, p. 509).

Mientras que, en el ámbito de la Defensa Nacional, la producción de Inteligencia se basó en temas referidos a: “Presencia Militar Extra Regional, Capacidades y Potencial Militar de otros Estados, Conflictos Armados y Recursos Naturales, Ciberdefensa y Contrainteligencia Defensivo Militar.” (Jefatura de Gabinete de Ministros: 2016, p. 509).

A su vez, la DINIEM concentró sus actividades de inteligencia en el ciberespacio a modo de responder a los pedidos explícitos de la Dirección de Ciberdefensa.

A lo largo de este título se ha desarrollado la evolución de la participación de los diferentes organismos de inteligencia en el ciberespacio, analizando específicamente aquellos con incidencia en la defensa nacional.

⁷ Bullentini, A. (1 de diciembre de 2015). “Predecir y prevenir ciberataques”, en Página 12 (consultado el 25 de noviembre de 2020 en <https://www.pagina12.com.ar/diario/elpais/1-287308-2015-12-01.html>)

Y si bien la DINIEM fue el primer organismo en iniciar los análisis sobre las cuestiones vinculadas al ciberespacio, el Ministerio de Defensa, a través de sus Directivas Políticas de Defensa Nacional de 2014 y 2018, pudo establecer definiciones precisas de lo que significa el ciberespacio en el marco militar, aunque dicha definición haya mutado de una DPDN a la otra, sin significar por ello un cambio de visión profundo.

Cuando estudiamos la participación del sistema de inteligencia argentino en el ciberespacio, se observa que este comienza a partir del año 2013, cuando al Ministerio de Defensa fue víctima de un ciberataque que alcanzó la seguridad de sus documentos confidenciales.

Con la llegada de la normativa implementada en el 2015 se puso de manifiesto la necesidad de abordar la ciberdefensa y la ciberseguridad por parte de los organismos de inteligencia.

Ahora bien, al contar con todas estas definiciones y específicamente entender la organización detallada (con sus responsabilidades y funciones), es que resulto posible iniciar el abordaje al tema, específicamente en el ámbito militar.

Conclusiones parciales

Como se dijo anteriormente el EMCO cuenta con un Comando de Ciberdefensa Conjunto y a su vez cada Fuerza con una Dirección de Ciberdefensa Especifica. Pero si entendemos que el ciberespacio no entiende de límites, de espacios, o de niveles; es que surge la inquietud desde la necesidad de contar con elementos de inteligencia que puedan dar respuesta a las necesidades de los comandantes en el nivel Táctico, ya que en los otros niveles se cuenta con estructuras y personal capacitado para la ejecución de dicha actividad.

Es así que se analizará la necesidad de contar con elementos de inteligencia en apoyo a una Gran Unidad de Combate (GUC), tratando de determinar si fuere necesario contar con organizaciones específicas o sólo contar con personal capacitado dentro de las organizaciones existentes.

CAPÍTULO III: EL CIBERESPACIO, EL NIVEL TÁCTICO Y LA COMPAÑÍA DE INTELIGENCIA

Cuando se analiza el ciberespacio, específicamente su injerencia en el desarrollo de las operaciones militares, se entiende que las actividades ejecutadas por las fuerzas militares se desarrollan en todos los tipos de conflicto, producto de que este ambiente es transversal a todos los demás y no entiende de espacios ni fronteras. A su vez esa transversalidad se aprecia en las diferentes fases de una operación, como así también en los diferentes niveles de la conducción.

Al poder desarrollarse un sin número de tipos de ataques (tantos como tipos de sistema que existan) y tan disimiles como un acceso no autorizado, o la captura de información sensible o la destrucción física de una instalación, es que un comandante debe procurar poseer una conciencia situacional que le permita comprender los alcances de los efectos que dichos ataques pueden producir sobre su capacidad para alcanzar los diferentes objetivos.

Mucho se ha analizado sobre la naturaleza de los ciberataques y su potencialidad dentro del nivel estratégico y por consiguiente las consecuencias que pueda traer aparejado como ser la de generar riesgos políticos no deseados.

Lo que conduce a entender que no siempre este tipo de operaciones deben ser ejecutada, o al menos no sin un profundo análisis de todo el espectro de consecuencias que conlleve desarrollar acciones de este tipo, ya que, no solo los elementos militares pueden ser engañados, destruidos o neutralizados, sino que también los elementos civiles de los sistemas de información del enemigo, tales como la banca, el comercio, el transporte y los medios de comunicación.

Pero a su vez, también es cierto que este tipo de operaciones no son exclusivas del nivel estratégico, ya que la amplia gama de dispositivos que utilizan el ambiente cibernético para cumplir su función son utilizados en todos los niveles y por consiguiente pueden ser vulnerables generando efectos de menor a mayor alcance de acuerdo al nivel que estén siendo empleados.

Maren Leed⁸ analiza los factores que ayudan a entender las diferencias entre los ciber-objetivos estratégicos y los operacionales y tácticos.

Lo que sucede es que cuanto más "estratégicos" sean los objetivos, es decir, de los que se pueden esperar efectos más importantes sobre el adversario o que podrían resultar decisivos en el curso de conflicto, es más probable que estén conectados vía un cable. Se trata de grandes redes de mando y control nacionales y su infraestructura de apoyo. Estos objetivos suelen también ser relativamente fijos y probablemente bien defendidos en los dominios de la física y la cibernética. Pero los comandantes de menor nivel que tal vez deseen utilizar las cibercapacidades en un sentido más limitado (por ejemplo, para denegar las comunicaciones locales por un período limitado de tiempo, interrumpir un carril de maniobra cerrando las señales de tráfico en una porción de una ciudad, o suprimir un sistema de dirección de armas tácticas) pueden ser más propensos a buscar afectar a las redes inalámbricas o blancos que dependen de una red local más circunscrita.

⁸ Leed, Maren; "Offensive Cyber Capabilities at the Operational Level: The Way Ahead" Center for Strategic and International Studies (CSIS), disponible en: https://csisprod.s3.amazonaws.com/s3fspublic/legacy_files/files/publication/130916_Leed_OffensiveCyberCapabilities_Web.pdf

Mientras que si continuamos el análisis de ataques que hayan afectado decisiones tácticas nos encontramos con el trabajo realizado por Parks y Duggan⁹ quienes afirman que:

Existen ejemplos de ataques que han afectado tanto a quienes toman decisiones tácticas como estratégicas. Las primeras pueden estar relacionadas con el engaño respecto de la ubicación y el tamaño del enemigo y de las fuerzas amigas. En el nivel operacional, el tiempo de arribo y cantidad de suministros y refuerzos podría ser manipulado para provocar decisiones erróneas como, por ejemplo, atacar con escasa munición o retener un ataque por temor a la falta de suministros. Tampoco hay que desechar, el caso de que quienes toman decisiones estratégicas puedan ser engañados por atribuir las acciones a otros países o grupos distintos al atacante real.

Es fácil apreciar en dicho trabajo que el conflicto en el ciberespacio se sucede en los tres niveles y fiel a la característica distintiva de transversalidad es que los interconecta de forma interactiva y sistémica.

Mientras que el nivel estratégico, debe brindar el marco legal y los límites que provean a los comandantes operacionales los objetivos a lograr en el ambiente del ciberespacio y los instrumentos disponibles para alcanzar dichos objetivos. En el nivel táctico, los comandantes deben combatir utilizando no sólo medios cinéticos, sino que también instrumentos cibernéticos ofensivos y defensivos.

⁹ Parks, Raymond C.; Duggan, David P.; "Principles of Cyber-warfare" Proceedings of the 2001 IEEE Workshop on Information Assurance and Security United States Military Academy, West Point, NY, 5-6 June, 2001. Disponible en: <http://opendawn.com/ewar/docs/dissertationsources/educationalsource2.pdf>

La doctrina dicta que los tres niveles se solapan durante la ejecución de una operación militar y esto no es ajeno al ambiente del ciberespacio.

Es decir que, "los comandantes y su personal en todos los niveles deben anticipar cómo sus planes, operaciones y acciones pueden afectar a los otros niveles. El nivel operacional vincula la estrategia y táctica mediante el establecimiento de objetivos operacionales necesarios para alcanzar el estado final militar. Secuencia las acciones tácticas para lograr los objetivos estratégicos."(MFE 1-01, CEDOE 2016)

Si entendemos que desde la perspectiva de que cualquier "nodo" específico podría ser objeto de un ataque cibernético particular, cualquier potencial objetivo teóricamente podría ser estratégico, operacional o táctico, según el propósito para el cual es utilizado y por quién.

En todos los niveles, el objetivo de los ciberataques es negar, interrumpir o degradar las capacidades enemigas, directa o indirectamente. Es así entonces que los comandantes de nivel táctico son más proclives a emplear ataques cibernéticos como parte de sus actividades en apoyo de su esquema de maniobra o de fuegos y enfrentarse a blancos fugaces que son difíciles de prever de antemano.

Entender entonces que las operaciones en el ciberespacio no se encuentran atadas exclusivamente a un nivel específico de la conducción, y por sobre todo comprender qué tendencias de empleo en dicho ambiente utilizan los comandantes del nivel táctico nos ayudan a materializar el tipo de apoyo de inteligencia que se requiere a este nivel y por consiguiente la necesidad de contar con un elemento capacitado, organizado y equipado para dar respuesta a esos requerimientos propios del nivel de conducción analizado.

Siendo la Compañía de Inteligencia el elemento de apoyo del nivel Gran Unidad de Combate (GUC), decanta, en un análisis preliminar, que debe ser el elemento responsable de poder responder a los requerimientos del comandante para ejecutar las acciones en el ciberespacio.

Como se describió anteriormente, las acciones que se pueden desarrollar varían de acuerdo con la variedad de sistemas que utilicen el ciberespacio para cumplir sus funciones.

Conclusiones parciales

Entender de las capacidades del enemigo para ejecutar operaciones en el ciberespacio, analizar cómo ellas pueden incidir sobre el desarrollo de las propias operaciones, vigilar dicho ambiente a modo de poder dar una alerta temprana, estudiar el ambiente y sus actores respectivos no son más que las mismas actividades que se desarrollan en el ambiente terrestre y poseen el mismo valor esencial para generar conciencia situacional y contribuir al proceso de toma de decisiones.

Es posible afirmar entonces que el elemento de inteligencia en apoyo al nivel GUC puede ser responsable de brindar el apoyo en el ciberespacio, pero primero para ello debe adecuar su organización (Cuadro de Organización), asignar personal formado dentro de inteligencia y especializado en este tipo de ambiente y asignar los medios materiales para que sea apta para el desarrollo de operaciones en dicho ambiente.

CONCLUSIONES FINALES

A lo largo del trabajo se han analizado principalmente tres conceptos que nos permitirán dar respuesta a nuestra hipótesis de análisis.

Primero se ha analizado el concepto de ciberespacio, y se ha tratado de determinar la pertinencia como un nuevo ambiente en el cual desarrollar las operaciones militares, llegando a definir el mismo, de acuerdo a lo establecido por la Directiva Política de Defensa Nacional (año 2014) como un ámbito transversal a los escenarios tradicionales de conflicto (mar, tierra, aire y espacio exterior), siendo ésta primera vez que Argentina definía conceptualmente al ciberespacio desde la óptica de la Defensa Nacional. Dicha conceptualización sería modificada en la siguiente DPDN del año 2018, la cual se refiere al ciberespacio como un quinto dominio de guerra.

Una vez definido que nos encontramos frente a un ambiente donde también se desarrollan las operaciones militares, es que se analizó la presencia, el marco legal y la evolución de los diferentes actores del Sistema de Inteligencia Nacional, definiendo responsabilidades y funciones, haciendo hincapié en la necesidad de contar con elementos de inteligencia que operen en este ambiente.

Se cree conveniente, abocarse específicamente a aquellas que atañen a la defensa nacional, pero sin dejar de explicar brevemente aquellas otras que coexisten dentro del sistema y operan en otros ámbitos (seguridad interior) ya que solo se puede ser eficiente cuando hay un trabajo armonioso y coordinado entre las mismas.

La Agencia Federal de Inteligencia (AFI), la Dirección Nacional de Inteligencia Estratégica Militar (DINIEM), el Ministerio de Defensa (MINDEF), el Comando Conjunto de Ciberdefensa y las

Direcciones de Ciberdefensa específicas de cada Fuerza son los elementos que actualmente tienen injerencia dentro de la defensa nacional en este nuevo ambiente del Ciberespacio.

Por último, se ha analizado la transversalidad de este ambiente específico sobre los diferentes niveles de la conducción para determinar la pertinencia de contar con elementos de inteligencia capacitados para operar en el ambiente cibernético en el nivel más bajo: el táctico.

Como se ha podido apreciar, las operaciones se desarrollan en todos los niveles, lo que cambia son los efectos que se buscan en cada uno de ellos y el tiempo de planeamiento previo a la ejecución de una operación.

Es por estas similitudes en el ambiente terrestre que se considera necesario contar con elementos de inteligencia que puedan dar respuesta a los requerimientos del comandante sobre este ambiente específico que influye sobre el normal desarrollo de las operaciones.

Entendiendo que el nivel táctico, específicamente donde desarrolla las operaciones la GUC, cuenta con un elemento de inteligencia en apoyo (la Compañía de Inteligencia), es que no se considera necesario la creación de un nuevo elemento, sino el análisis del cuadro de organización que permita agregar a dicha subunidad las funciones de apoyo en el ambiente cibernético; proporcionándole personal formado en inteligencia y perfeccionado para el desarrollo de las funciones en dicho ambiente, además de contar con el equipamiento necesario para el cumplimiento de la misión.

BIBLIOGRAFÍA

Albarracín Keticoglu, Ana y Sergio Eissa. (2019). Ciberdefensa en Argentina. Pujas en torno a su definición.

Carrillo Robles, Margarita. (2015). Amenaza y uso de la fuerza a través del ciberespacio.

Sol Gastaldi y Leandro Ocón (Eds.), Ciberespacio, Estrategia y Defensa Nacional, mimeo, Buenos Aires, Argentina.

Dougherty, James y Robert Pfaltzgraff. (1993). Teorías en pugna en las Relaciones Internacionales. Argentina: GEL. ISBN: 950-694-292-7.

Ganuza Artiles, N. (2010). Situación de la ciberseguridad en el ámbito internacional y en la OTAN.

Joyanes Aguilar, L. Cuadernos de Estrategia N° 149. Ciberseguridad: retos y amenazas a la Seguridad Nacional en el ciberespacio, (pp 166 - 214), España: IEEE.

Alfaomega. Kent, S. (2016). Strategic Intelligence for American World Policy, United States: Princeton Legacy Library.

Kuehl, Daniel (2009) From Cyberspace to Cyberpower: Defining the Problem.

Harley, Matthew (2014) Looking Back, Thinking Ahead: C2 and ISR for the Information Age

Paper presented at the Mitchell Institute for Aerospace Studies, Rosslyn, VA · 1 sept. 2014

Franklin D. Kramer, Stuart H. Starr, y Larry K. Wentz (Eds.), Cyberpower and National Security (pp 24-42). Washington, DC: Center for Technology and National Security Policy, National Defense University, Potomac Books, Inc. ISBN: 978-59797-423-3.

Li, J. and Daugherty, L. (2015). Training Cyber Warriors: What can be learned from defense language training? California, United States: Rand Corporation.

Taleb, N. (2018). El cisne negro. El impacto de lo altamente improbable. Buenos Aires, Argentina: Paidós.

MINDEF. (2015). Libro blanco de la defensa. Buenos Aires, Argentina: MINDEF.

Decreto 2645 / 2014. Apruebase la actualización de la “Directiva de Política de Defensa Nacional” (DPDN) que, como Anexo I, forma parte del presente. 19 de Enero de 2015.

Decreto 703 / 2018. Apruebase la “Directiva de Política de Defensa Nacional” (DPDN). Deroganse el Decreto N° 1714 del 10 de noviembre de 2009 y el Decreto N° 2645 del 30 de diciembre de 2014. 31 de Julio de 2018.

Decreto 2690 / 2014. Apruebase la “Directiva de Política de Defensa Nacional” (DPDN). Deroganse el Decreto N° 1714 del 10 de noviembre de 2009 y el Decreto N° 2645 del 30 de diciembre de 2014. 31 de Julio de 2018.

Jefatura de Gabinete. (2014). Memoria Detallada del Estado de la Nación 2013.

Jefatura de Gabinete. (2016). Memoria Detallada del Estado de la Nación 2015.

MFE 1-01 (2016) Doctrina, Centro de doctrina del Ejército, Fuerzas Militares de Colombia

Ejército Argentino (2015). Conducción para las Fuerzas Terrestres (ROB – 00 – 01).

Marcelo de los Reyes. (2018). La inteligencia estratégica como instrumento fundamental para la toma de decisiones. Recuperado de <https://es.scribd.com/document/392354912/La-Inteligencia-Estrategica-comoinstrumento-fundamental-para-la-toma-de-decisiones>

Bullentini, A. (1 de diciembre de 2015). “Predecir y prevenir ciberataques”, en Página 12. Recuperado de [https://www.pagina12.com.ar/diario/elpais/1-287308-2015-](https://www.pagina12.com.ar/diario/elpais/1-287308-2015-12-01.html)

12-01.html CCDCOE. “About us”. Recuperado de <https://ccdcOE.org/about-us/> CCDCOE. (24-28 Apr 2017). Locked Shields 2017. Recuperado de: <https://ccdcOE.org/locked-shields-2017.html> CISCO.

Puente, M. L. (1 de abril de 2018). Guía para entender la nueva geopolítica del ciberespacio. Perfil. (Consultado el 5 de diciembre de 2018 en <https://www.perfil.com/noticias/elobservador/guia-paraentender-la-nueva-geopolitica-del-ciberespacio.phtml>).

Miguel, H. (15 de marzo de 2018). Mitos y realidades de la ciberdefensa. Revista DEF (consultado el 6/12/2018 en <http://defonline.com.ar/mitos-y-realidades-de-la-ciberdefensa/>).

Leed, Maren; “Offensive Cyber Capabilities at the Operational Level: The Way Ahead” Center for Strategic and International Studies (CSIS), disponible en: https://csisprod.s3.amazonaws.com/s3fspublic/legacy_files/files/publication/130916_Leed_OffensiveCyberCapabilities_Web.pdf.

Parks, Raymond C.; Duggan, David P.; “Principles of Cyber-warfare” Proceedings of the 2001 IEEE Workshop on Information Assurance and Security United States Military Academy, West Point, NY, 5-6 June, 2001. Disponible en: <http://opendawn.com/ewar/docs/dissertationsources/educationalsource2.pdf>