MATERIA: TRABAJO FINAL INTEGRADOR

TEMA:

Ciberoperaciones

TÍTULO:

La visualización de un marco referencial para el Nivel Operacional

AUTOR: My Cristian Ariel Grogovinas

PROFESOR: Migue**l** Gratacos.

Año 2018

1. Resumen.

El eje central de este trabajo gira en torno a visualizar los vacios resultantes de confrontar el marco legal en la República Argentina con el desarrollo y empleo de capacidades que se consideran necesarias emplear en el Ciberespacio como producto del análisis de casos de relevancia a nivel mundial, donde el ambiente operacional propio del nivel de interés, se vio alterado, evidenciando el potencial del empleo de medios en esta nueva dimensión y su alcance en cuanto a la incidencia en la conducción de las operaciones militares.

Inicialmente se señalan las actividades que se desarrollan en el ciberespacio, con sus características particulares y el planteo de nuevos paradigmas frente al marco legal vigente en la República Argentina de aplicación para el empleo de las Fuerzas Armadas, que fue concebido cuando aún no existía el concepto de ciberespacio como un área de alto impacto e influencia en la resolución de conflictos.

A posterior se analiza cual es el estado del arte en función a documentos doctrinarios disponibles en fuentes abiertas como la Directiva de Ciberdefensa 2015 del Departamento de Defensa de los Estados Unidos, la Doctrina Gerasimov de las fuerzas armadas rusas, y la ley de Ciberseguridad de Lituania, como analogía a un hipotético escenario hibrido –casos Ucrania y Estonia - para enfrentar la concepción rusa de las nuevas formas de hacer la guerra, donde el empleo de ciberoperaciones para alterar el status quo del Ambiente Operacional ha tenido un alto impacto, a fin de establecer conclusiones parciales de interés que integradas a los aspectos resultantes en la primer parte del trabajo, permiten sentar lineamientos para un marco referencial particular del Nivel Operacional.

1.1 Palabras clave.

Ciberdefensa, Ciberoperaciones, Ciberespacio, Ambiente Operacional.

Agradecimientos

A mi madre María Elena por su apoyo incondicional durante esta etapa académica de mi carrera militar.

Introducción

Justificación del problema

La evolución del arte de la guerra, presenta formas que traen aparejados nuevos paradigmas a resolver.

La aparición del ciberespacio como un nuevo dominio con características propias que se suma a los ya conocidos (espacio, aire, tierra y mar), y los escenarios de los conflictos contemporáneos en los que intervienen actores estatales y no estatales persiguiendo intereses de variada naturaleza, donde los hechos muestran que pueden escalar de manera abrupta las etapas de un conflicto, imponen la necesidad de analizar los nuevos desafíos para el instrumento militar. En la actualidad no existe un consenso global respecto del empleo militar del ciberespacio al tiempo que son escasos los antecedentes que en torno al nivel operacional. Asimismo, la mayor parte de los escritos disponibles a través de fuentes abiertas es en idioma inglés.

Las guerras hibridas, donde las acciones no se limitan al enfrentamiento de ejércitos regulares, y donde la asimetría que las caracteriza, como así también el accionar sobre las condiciones del ambiente operacional, los factores que la componen, en especial el ambiente geográfico y su población en forma directa o indirecta a través de acciones que transforman el entorno con un esfuerzo relativamente bajo en función del alcance de los efectos, requieren de un nuevo enfoque para mantener el status quo inicial o el logro de condiciones más favorables para el desarrollo de operaciones en el nivel operacional.

Las consecuencias sistémicas de los efectos que se generan en el ciberespacio o a través del mismo, especialmente sobre la infraestructura crítica y la posición de la sociedad, tienen la capacidad de transformar radicalmente el ambiente operacional en un lapso breve de tiempo, condicionando la ejecución de las operaciones planificadas, o bien proporcionando ventajas al constituirse en un multiplicador del poder de combate.

El marco legal contemporáneo, que separa Defensa y Seguridad Interior, al tiempo que regula la actividad de Inteligencia en el mismo sentido sumado a los vacios doctrinarios existentes en la República Argentina para las actividades que se desarrollan en el ciberespacio, ¿permite al Nivel Operacional abordar esta problemática de forma integral y eficiente, a la luz de la evolución del estado del arte que se refleja en casos de relevancia a nivel mundial donde las condiciones del ambiente operacional se vieron

afectadas de forma precipitada con consecuencias sistémicas que van más allá incluso de las operaciones militares propiamente dichas ?

Planteo o Formulación del problema

El problema formulado se define como la necesidad de establecer lineamientos para un marco referencial del nivel operacional en el ámbito del ciberespacio, ante la existencia al día de hoy de un estado pre doctrinario donde lo que se ha escrito no ha sido aún formalizada.

Para ello es necesario dar respuesta a los siguientes interrogantes:

¿Es adecuado el marco legal vigente en la República Argentina para el desarrollo de capacidades acordes con la naturaleza de la actividad en el ciberespacio en el nivel operacional?

¿Cuáles son las capacidades necesarias para emplear en el ciberespacio a fin de preservar o modificar favorablemente las condiciones del ambiente operacional?

¿Cómo hacer frente a amenazas cibernéticas de origen incierto que pudieran afectar la infraestructura critica del país?

¿Es necesario ampliar la visión que plantea la Ciberdefensa para desarrollar acciones preventivas en el ciberespacio y/o a través del mismo?

Objetivos de la investigación

Objetivo general: visualizar un marco referencial para el desarrollo de Ciberoperaciones en el Nivel Operacional

Objetivos específicos.

Objetivo específico Nro 1: analizar el marco legal vigente en la República Argentina y las limitaciones implícitas para con la naturaleza de las operaciones en el ciberespacio

Objetivo específico Nro 2: identificar el alcance de las Ciberoperaciones y su incidencia en las condiciones del ambiente operacional, a la luz de casos de relevancia mundial.

Objetivo específico Nro 3: analizar las tendencias doctrinarias según las concepciones en el marco de la OTAN, Rusia y EEUU.

Marco teórico

El presente TFI, tiene sus bases teóricas en la Ley de Defensa y su decreto correspondiente, y aquellas partes de la Ley de Seguridad Interior e Inteligencia donde entiende el ámbito de Defensa en las condiciones que regula el marco legal vigente, no obstante la ausencia de doctrina militar conjunta o especifica que especifique para el nivel operacional los aspectos que en relación al ciberespacio, enumera la Directiva Política de Defensa Nacional 2018. Se analiza el Decreto 577/2917 para la creación de un Comité de Ciberseguridad en la órbita del Ministerio de Modernización -también integrado por representantes del Ministerio de Defensa, y el ministerio de Seguridad- el cual tiene por objetivo la elaboración de una Estrategia Nacional de Ciberseguridad.

Asimismo, se recurrirá a fuentes bibliográficas, fuentes abiertas y documentos nacionales derivados de doctrina extranjera de carácter público, que establezcan lineamientos de la evolución del estado del arte en el mundo, a la luz de conflictos contemporáneos y hechos significativos que abordan la problemática que plantea al ámbito militar el ciberespacio, para suplir el vacio doctrinario existente en nuestro país.

También se tomarán como bases teóricas los conceptos vertidos en las dictadas durante el ciclo 2018 en la ESGC, particularmente Acción Militar Conjunta e Inteligencia Operacional.

Finalmente, se establecerán conclusiones; en primer término con un carácter crítico producto de confrontar los contenidos legales para la Defensa en vigencia en la República Argentina, con la naturaleza de la actividad, para buscar visualizar del análisis de casos contemporáneos, las capacidades y condiciones necesarias para las ciberoperaciones en el nivel operacional que permitan una aproximación al establecimiento de lineamientos para un marco referencial del nivel de interés.

Metodología empleada

Explicación sobre el método empleado

El presente TFI, se inicia con un análisis general para luego ir a lo particular de los objetivos específicos. La ausencia de una doctrina conjunta o especifica en la actualidad, hacen necesario recurrir a fuentes que permitan analizar sobre la base de distintas ópticas, cual es el estado del arte a la luz de casos relevantes donde se ven reflejados indicios a los interrogantes planteados.

Asimismo, a través de dichos documentos extraer conceptos relevantes para esta investigación reflejados en casos de conflictos de naturaleza hibrida donde se evidencia

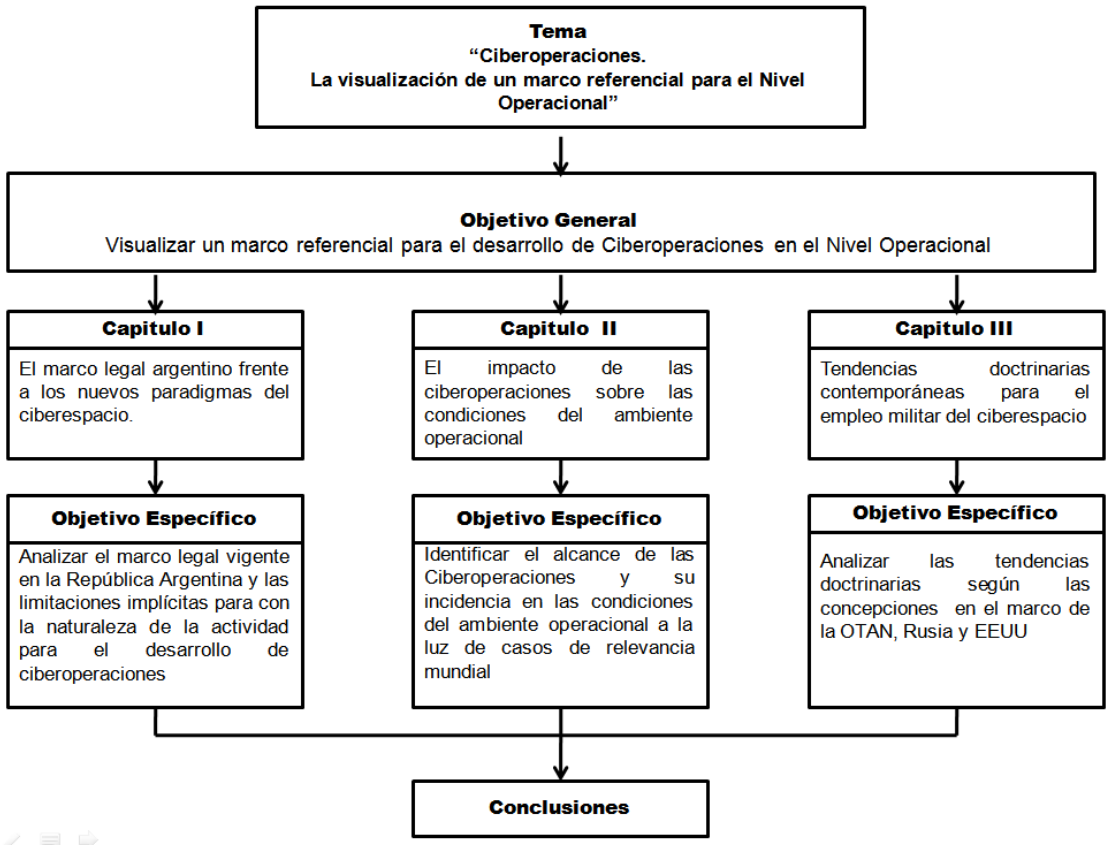
el alto impacto de las ciberoperaciones, para establecer conclusiones, que sirvan de sustento los fundamentos propuestos al final del TFI.

La finalidad es visualizar lineamientos para un marco referencial en el nivel operacional en el desarrollo de ciberoperaciones.

El diseño

Se utilizará método exploratorio, en función de analizar los objetivos específicos que se establecen para cada capítulo del presente trabajo, a través del análisis bibliográfico y documental.

Esquema Gráfico Metodológico



Capítulo I: El marco legal argentino frente a los nuevos paradigmas del ciberespacio

En la República Argentina se establece una diferenciación conceptual en cuanto a Defensa Nacional y Seguridad interior, a través de las leyes 23.554; 24.059, y el Decreto 703/2018 correspondiente a la Directiva Política de Defensa Nacional (DPDN) de interés para el presente trabajo. Por consiguiente el concepto de "Seguridad Nacional" que en otros países integra esos dos ámbitos, no es de aplicación. Se considera un dato de relevancia para abordar en el desarrollo de este capítulo los límites establecidos en materia de Defensa, y el alcance de la naturaleza de las actividades que se desarrollan en el Ciberespacio por parte de los actores estatales y no estatales que responden a un amplio abanico de intereses y exentos del ámbito de competencia del instrumento militar del país, pero que no obstante la generación de efectos en tiempos de paz o de conflicto, podrían incidir en el ámbito de la Defensa dada la amplitud de factores que componen el ambiente operacional donde se desarrollarán las operaciones militares.

La Ley de Defensa Nacional 23.554 y los límites que establece.

La Ley 23.554 (1988), establece las bases jurídicas, orgánicas y funcionales para la preparación, ejecución y control de la defensa nacional de la República Argentina.

El artículo 2, señala que "*la defensa nacional es la integración de la acción coordinada de todas las fuerzas de la Nación para la solución de aquellos conflictos que requieren el empleo de las Fuerzas Armadas, en forma disuasiva o efectiva para enfrentar las agresiones de origen externo. Tiene por finalidad garantizar de modo permanente la soberanía e independencia de la Nación Argentina, su integridad territorial y capacidad de autodeterminación; proteger la vida y libertad de sus habitantes*" (Honorable Congreso de la Nación [HCN], 1988)

Se limita a través de este artículo a "agresiones de origen externo", lo cual se amplía por el decreto que reglamenta la Ley de Defensa a partir del año 2018, sean estos actores estatales o no.

El artículo 4, establece que "para dilucidar las cuestiones atinentes a la defensa nacional, se deberá tener permanentemente en cuenta la diferencia fundamental que separa la defensa nacional de la seguridad interior. La seguridad interior será regida por una ley especial". (HCN, 1988)

Por su parte, el artículo 15, establece que "las cuestiones relativas a la política interna del país no podrán constituir en ningún caso hipótesis de trabajo de organismos de inteligencia militares", aspecto no menor considerando la dificultad que existe para establecer el origen y autoría de las acciones en el ciberespacio. (HCN, 1988)

El Articulo 5, establece que "*la defensa nacional abarca los espacio continentales, Islas Malvinas, Georgias y Sandwich del Sur, y demás espacios insulares, marítimos y aéreos de la República Argentina, así como el sector antártico argentino, con los alcances asignados por las normas internacionales, y los tratados suscriptos o por suscribir por la Nación esto sin perjuicio de lo dispuesto por el artículo 28"* (HCN, 1988)*;* por su parte el artículo 28 de dicha ley, establece que para el caso de guerra o conflicto armado internacional *"*el Presidente de la Nación podrá establecer teatros de operaciones, delimitando las correspondientes aéreas geográficas" (HCN, 1988)

De estos artículos, se resalta el concepto, de un espacio definido, con límites geográficos, que en la doctrina nacinal da lugar al concepto de teatro de operaciones, mientras que el concepto de ciberespacio hace referencia a una dimensión que atraviesa los espacios físicos ya conocidos.

Decreto 703. Directiva Política de Defensa Nacional (DPDN) 2018. Conceptos de interés

Existen aspectos referidos al ámbito del ciberespacio que se consideran de interés extraer del contenido de la DPDN 2018 para el presente trabajo, ya que en ella se establecen los lineamientos de la política de Defensa del país.

En cuanto al análisis del escenario global, se indica la preeminencia del poder militar de Estados Unidos, China y Rusia, como así también el crecimiento de la autonomía de actores estatales y no estatales de diverso poder relativo y atributos de poder. Y que los actores no estatales promovidos por otras naciones y/o grupos de poder, cuentan con la capacidad de disputar el monopolio de la violencia estatal, impactando en las políticas internaciones asociadas al ciberespacio.

Que la disuasión toma un protagonismo relevante, en la ampliación de las doctrinas militares al ciberespacio ante la necesidad de hacer frente a amenazas tradicionales y no tradicionales; menciona el uso de información falsa, ejércitos privados reemplazando a los regulares, el uso y explotación del ciberespacio por parte de actores no estatales, donde las mayores amenazas por su grado de sofisticación siguen teniendo su origen en actores estatales.

Para el área de Defensa, se plantea que la problemática tiene su foco en salvaguardar la infraestructura crítica del Sistema de Defensa Nacional y de toda aquella que designe el nivel político para su preservación.

Respecto de la utilización del ciberespacio con fines militares, reafirma la consolidación del mismo como un ambiente más para la defensa, dadas las amenazas que podrían afectar intereses estratégicos para el país. Y agrega sobre la existencia de operaciones de agresión e influencia sobre las naciones adversarias, con lo cual surge la necesidad de adecuar las organizaciones de la República Argentina, orientándolas a la reducción de vulnerabilidades que resultan de la informatización de activos estratégicos de interés para la Defensa Nacional, en un marco de cooperación interestatal y del empleo de capacidades materiales, infraestructurales y tecnológicos en apoyo a una estrategia integral para las problemáticas de esta naturaleza, que se corresponden con organismos de seguridad pública e inteligencia nacional y criminal.

Respecto del Instrumento militar, establece que su empleo será disuasivo o efectivo "*ante conflictos originados por agresiones de origen externo contra espacios de jurisdicción nacional, la soberanía, la integridad territorial, la capacidad de autodeterminación de la República Argentina y la vida y libertad de sus habitantes, o ante cualquier forma de agresión contemplada en la Carta de las Naciones Unidas, sin perjuicio de lo establecido en la Ley N° 24.059 de Seguridad Interior."* (HCN, 2018)

Asimismo que se priorizará, en tiempo de paz, el desarrollo de operaciones de Protección de Objetivos Estratégicos y Apoyo al Sistema de Seguridad Interior, entre otros, siendo estos aspectos de relevancia para el foco de este trabajo. En cuanto a la oportunidad, hace referencia a "estadios de paz y crisis". Y en cuanto a la responsabilidad del Ministerio de Defensa, expresa que la misma es la de "*conducir y establecer los lineamientos y prioridades de nivel operacional para garantizar la seguridad de los activos digitales e infraestructuras informáticas críticas de la Defensa Nacional y de aquellos que les asigne el Poder Ejecutivo Nacional (PEN) en contribución a la seguridad estratégica de la Nación.*" (HCN, 2018)

De los conceptos extraídos, se aprecia la consideración de actores no estatales que tienen intervención en el ciberespacio, ámbito para el cual el instrumento militar debe adecuar sus organizaciones, la necesidad del desarrollo de actividades interagenciales para el eficaz empleo de los medios del instrumento militar en operaciones de apoyo a la seguridad interior y la protección de infraestructura critica vital para el país. La apari-

ción de actores no estatales que pudieren ser fuente de agresión sobre Objetivos de Alto Valor Estratégico (OVAE), permite afirmar de la aparición de nuevos paradigmas donde las reglas de juego que establece el marco legal, podrían carecer de la flexibilidad necesaria para neutralizar los efectos en oportunidad en virtud del grado de dificultad para identificar la autoría, objetivos e interés.

Decreto 683/2018. Conceptos de Interés

El presente decreto, que reemplazó al anterior Decreto 727/2006, que como aspecto más relevante para el presente TFI sobresale el carácter restrictivo limitaba el empleo de las FFAA a amenazas estatales de origen externo

El decreto 683/2018, sustituye varios artículos del mencionado, ampliando el empleo de las FFAA a amenazas de origen externo- eliminando el termino estatales- contra la soberanía, la integridad territorial o la independencia de la política, la vida y la libertad de sus habitantes o ante cualquier otra forma de agresión externa que sea compatible con la Carta de las Naciones Unidas.

Asimismo deja establecido que no queda afectado lo dispuesto en la Ley 24.059 de Seguridad Interior, en lo concerniente a los escenarios en los que se prevé el empleo de las FFAA y a las disposiciones que definen el alcance de dicha intervención en operaciones de apoyo a la Seguridad Interior. (HCN, 2018)

El Articulo 3, enmarca el planeamiento y empleo a los tipos de operaciones que pueden realizar las FFAA; Defensa de Intereses Vitales, Operaciones en el Marco de la ONU, las encuadradas en la Ley de Seguridad Interior, Apoyo a la Comunidad Nacional e Internacional, conforme con las limitaciones previstas para la Seguridad Interior, y mencionada la Ley de Inteligencia Nacional Nro 25.520 (HCN, 2018)

El Artículo 24 bis, establece la custodia de los objetivos estratégicos al Sistema de Defensa Nacional, por parte de la Armada, Ejército y Fuerza Aérea, como integrantes del mismo, además de la Gendarmería Nacional y la Prefectura Naval Argentina. (HCN, 2018)

Para avanzar con el presente trabajo, se establece necesario, adoptar una definición para agresión cibernética, entendiéndola como una "*acción ofensiva, voluntaria o no, que se ejecuta en o a través del ciberespacio, sobre una infraestructura crítica o activo de información del sistema de defensa nacional y ocasiona, como consecuencia, daños a su disponibilidad, integridad y confidencialidad afectando el desarrollo de las operaciones que ejecuta en cumplimiento de su misión*" (Guimpel, 2018)

La Naturaleza de la actividad en el ciberespacio. Estado del Arte.

El vacío existente en cuanto a una doctrina conjunta para el nivel operacional, conduce a la necesidad de apoyarse en los conceptos que dicta el estado del arte en la actualidad u otras fuentes doctrinarias referenciales que permiten comprender los nuevos paradigmas que trae aparejado el surgimiento de una nueva dimensión que constituye un nuevo ámbito para el empleo de las FFAA, en concordancia con los lineamientos establecidos en la DPDN que establece la responsabilidad para el planeamiento sobre la protección de Objetivos de Valor Estratégicos y el apoyo a las operaciones de Seguridad Interior, cuando sea requerido por parte del Poder Ejecutivo Nacional.

Para el Departamento de Defensa de EEUU, el Ciberespacio es "un dominio global dentro del entorno de la información que consiste en una red independiente de infraestructuras de tecnologías de la información, incluyendo Internet, redes de telecomunicaciones, sistemas informáticos, procesadores embebidos y controladores"[1]

Para el General Brett Williams[2] Director de Operaciones del Ciber Comando de EEUU es "*el dominio artificial creado al conectar todos los ordenadores, conmutadores, enrutadores, cables de fibra óptica, dispositivos inalámbricos, satélites y otros componentes que nos permiten mover grandes cantidades de datos a velocidades muy rápidas. Al igual que en los dominios físicos, terrestre, marítimo, aéreo y espacial, en el espacio cibernético llevamos a cabo una variedad de actividades en beneficio de individuos, gobiernos y entidades comerciales. La diferencia clave entre los dominios físicos y el espacio cibernético es que el espacio cibernético es artificial y cambiante. Esta característica ofrece tanto oportunidades como riesgos*."

Brett, en cuanto al uso militar del espacio cibernético señala que, "si se concentra la atención en el nivel operacional de la guerra, se encuentra que las operaciones en el espacio cibernético son bastante similares a las operaciones que se llevan a cabo en los otros ámbitos". El espacio cibernético es un espacio operacional, como lo es el mar, el aire, la tierra y el espacio. Si el nivel operacional busca colocarse en la mejor posición

[1] Joint Publication (JP) 1-02, Department of Defense Dictionary of Military and Associated Terms

[2] Williams Brett T, The Joint Force Commander's Guide to Cyberspace Operations, Joint Force Quarterly 73, 2nd Quarter 2014, P. 14; Disponible en: http://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-73/jfq-73_12-19_Williams.pdf

para llevar a cabo los enfrentamientos, al espacio cibernético le cabe un papel importante en tal acción.

Para De Vergara y Trama[3] existe una ausencia de una acuerdo en cuanto a la terminología a emplear, e introduce el término "dominio", sosteniendo que "se entiende por dominio a los cinco ambientes donde se desarrollan los conflictos armados" (aire, mar, tierra, espacio y cibernético). Agrega que todos son reales, excepto el cibernético que es virtual. Y que "*que tiene características distintivas que requieren una doctrina especializada, una política de empleo, recursos estandarizados entre las Fuerzas Armadas y expertos en el tema. Debido a su reciente aparición, el espacio cibernético es más dificultoso de comprender porque no es fácil adentrarse en un espacio virtual, pero si se habla del nivel operacional de guerra*",

Para Casar Corredera[4] que aborda la problemática que plantea el ciberespacio como un nuevo espacio de confrontación, este nuevo dominio posee una serie de características particulares que establece de la siguiente manera estos conceptos:

- "*es un entorno único, en el que el atacante puede estar en cualquier parte del mundo.*
- *En la defensa intervienen muchos factores, y no sólo elementos estatales sino también privados. Se exige pues una estrecha coordinación entre todos ellos.*
- *La confrontación en el espacio cibernético presenta frecuentemente las características de un conflicto asimétrico; y es frecuentemente anónimo y clandestino.*
- *Permite obtener información sobre objetivos sin necesidad de destruir ni neutralizar ningún sistema y, a menudo, sin delatarse.*
- *Permite también ejercer el chantaje; pero, al mismo, tiempo, la defensa puede utilizarlo para la disuasión.*
- *Evoluciona rápidamente siguiendo la evolución tecnológica de las TIC."*

Ciberdefensa y Ciberoperaciones. Países y posturas.

[3] Vergara, E. & Trama, G. (2017). Operaciones militares cibernéticas: Planeamiento y Ejecución en el Nivel Operacional. Buenos Aires: Escuela Superior de Guerra Conjunta de las Fuerzas Armadas.

[4] Casar Corredera, José Ramón, "El Espacio cibernético: Nuevo escenario de confrontación", Centro Superior de Estudios de la Defensa Nacional, Monografías del CESEDEN, febrero de 2012, P. 14; Disponible en;
:http://www.defensa.gob.es/ceseden/Galerias/destacados/publicaciones/monografias/ficheros/126_EL_ESPACIO CIBERNÉTICO_NUEVO_ESCENARIO_DE_CONFRONTACION.pdf

En la República Argentina, se entiende por Ciberdefensa como "*el conjunto de acciones que se desarrollan en el ciberespacio para prevenir, detectar, identificar, anular, impedir, evitar, contrarrestar, contener o repeler una amenaza o agresión cibernética, sea esta inmediata, latente, o potencial, a fin de permitir el empleo del Instrumento Militar de la Nación*" (Guimpel, 2018).

La Argentina no tiene una definición legal de Seguridad, sino que definió Seguridad Interior con cierto grado sesgo respondiendo al contexto de naturaleza política de la época.

La diferencia que hace nuestro país separando en materia legal, Defensa y Seguridad Interior, es determinante en cuanto al ámbito de empleo de las fuerzas armadas frente a la aparición de una nueva dimensión con características particulares propias que no responden a reglas consensuadas, y que planteando interrogantes para el abordaje integral de este tipo de amenazas – tal es el caso de ciberataque contra infraestructura critica sensible y/o la percepción de la sociedad- con una autoría, intereses, objetivos y ubicación geográfica difíciles de distinguir con certeza.

Para el General de Brigada Paulo Carvalho[5] de Brasil, su país entiende a la Ciberdefensa como "*un conjunto de acciones defensivas, ofensivas y explotarías, llevadas a cabo en el espacio cibernético, en el contexto de una planificación de nivel estratégico nacional coordinado e integrado por el Ministerio de Defensa, para los fines de proteger los sistemas de información del país, obtener datos para la producción de conocimientos de inteligencia y comprometer la eficacia de los sistema de información del adversario*".

Se visualiza la diferencia entre la concepción de la Ciberdefensa, en la Argentina, donde posee un carácter pasivo, mientras que en Brasil, se consideran medidas ofensivas, y exploratorias donde particularmente estas últimas implican la ejecución actividades y tareas que involucran al campo de la Inteligencia Militar desde la paz, en pos de anticiparse a través de la producción de conocimientos ante potenciales actores que hagan uso del ciberespacio.

---

[5] Carvalho, Paulo Sergio, Defesa Cibernética e as Infraestruturas Críticas Nacionais, Anais Do X Ciclo De Estudos Estratégicos:
Proteção Das Infraestruturas Críticas, Disponible en:
http://www.eceme.ensino.eb.br/meiramattos/index.php/RMM/issue/view/15 El subrayado es nuestro

Por su parte en el Reino de España, que tiene una doctrina de Seguridad Nacional integrando lo que en la Argentina entendemos como Defensa y Seguridad Interior, la Ciberdefensa en el ámbito de sus Fuerzas Armadas tiene como objeto "Potenciar las capacidades militares y de inteligencia para ejercer la respuesta oportuna, legitima y proporcionada en el espacio cibernético ante amenazas o agresiones que puedan afectar a la Defensa Nacional" (Mando Conjunto de Ciberdefensa de España, 2018)

Se observa que en dichos países, existe un espectro más amplio para la Defensa y una necesidad atendida desde el campo militar que permite anticiparse a posibles escenarios a través del ciclo de producción de la Inteligencia, aspecto que desde nuestro marco legal posee un carácter restrictivo, teniendo su origen en el contexto político interno de cuando las respectivas leyes fueron promulgadas, y que a consecuencia de ello en la actualidad limitan el pleno desarrollo de capacidades para hacer frente de forma eficiente a los nuevos paradigmas resultantes del quinto dominio.

Para De Vergara y Trama (2017), que realizan un análisis de numerosas fuentes a fin de establecer un concepto que unifique distintos criterios escritos del tema, las Ciberoperaciones son "*todas aquellas operaciones ejecutadas para interrumpir, negar, degradar o destruir la información existente en las computadoras y redes de computadoras, o las computadoras y redes propiamente dichas; y pueden ser una forma avanzada del uso de la fuerza que precede el esfuerzo principal en el Teatro de Operaciones a fin de preparar el objetivo para el asalto principal*". Los mismos autores elaboran un concepto de Gestión de la Información Cibernética al cual definen como "*capacidad de recopilar y compartir información de forma que permita un intercambio rápido y fiable de esta entre diferentes partes. Entre la información de referencia sobre ciberdefensa a compartir, se encontrara una estimación de la intención del adversario y de su capacidad, así como información acerca de las vulnerabilidades conocidas, software malicioso, y las evaluaciones y certificaciones de los diferentes productos de software y hardware".* Se visualiza a través de la primer definición, una necesidad implícita de adecuar a favor, las condiciones del Ambiente Operacional al tiempo que por medio de la segunda, la necesidad de una fluidez interagencial en razón de lo difuso de los límites entre las aéreas ante la necesidad de hacer frente a una amenaza en el ciberespacio de la cual se desconoce su autoría e intención.

La Sorpresa, es uno de los principios que considera nuestra doctrina para la Acción Militar Conjunta para la conducción de las operaciones ya que "*busca accionar sobre el*

oponente en un lugar y momento o en una forma tal, para la que no se encuentre preparado. Implica retener la iniciativa y es una condición previa para el éxito. No necesariamente significa un accionar inesperado, sino que el oponente pese a darse cuenta de nuestra acción, no puede tomar medidas para evitarla" [6].

La sorpresa actúa como un multiplicador de poder de combate, permitiendo anticiparse a las acciones de un enemigo o bien obteniendo ventajas significativas. Se aprecia que la concepción de la Ciberdefensa focalizada en medidas netamente pasivas, dificulta la obtención de la misma a través de operaciones complementarias en el ciberespacio y que por lo tanto, en concordancia con la naturaleza de los actores y actividades que allí se ejecutan, es necesario el desarrollo de capacidades ofensivas que puedan ser empleadas en oportunidad.

Ciberataques a la infraestructura critica, guerra informativa y población. Matices de la Doctrina Gerasimov y la Guerra Hibrida.

Se entiende al Ambiente Cibernético como "*el conjunto de condiciones y características que existen en forma estable o semiestable en el ciberespacio y, consecuentemente, influyen sobre las infraestructuras críticas y activos de la información del Instrumento Militar y que, junto a otros elementos, forma parte del Ambiente Operacional.*" (Cicerchia, 2017)

Por su parte, la infraestructura critica, "*es el conjunto de instalaciones, redes, servicios, equipos físicos de tecnologías de la información y comunicaciones del Instrumento Militar de la Nación cuya interrupción o destrucción puede tener una repercusión importante en el desarrollo de las operaciones que ejecuta en cumplimiento de su misión.*"(Cicerchia, 2017)

Una amenaza cibernética, entendida en su esencia como una capacidad, puede ser desarrollada por un Estado, un individuo o grupo de individuos u una organización no estatal, los cuales podrían actuar sobre la infraestructura critica de un país alterando las

[6] Ministerio de Defensa; Estado Mayor Conjunto de la Fuerzas Armadas; República Argentina; Manual de Doctrina Básica para la Acción Militar Conjunta; PC 00 – 01; Proyecto 2013; Capítulo I; p.5.

condiciones del ambiente cibernético de forma sistémica y por consiguiente el ambiente operacional, en particular la población.

Los conflictos contemporáneos donde se ha visto el impacto de las operaciones cibernéticas a merced de la afectación de infraestructura crítica sensible para el funcionamiento de servicios esenciales son un ejemplo de transformación de las condiciones del Ambiente Operacional, lo cual fue acompañado por Operaciones de Información (explotando el uso de redes sociales y medios masivos de comunicación), Inteligencia y el empleo de Fuerzas Especiales, teniendo en todos los casos como objetivo la población a fin de alterar las condiciones del Ambiente Operacional y la voluntad de lucha. Se analizaran el caso de Ucrania, donde el empleo de la denominada Doctrina Gerasimov se puso en práctica por parte de Rusia, utilizando componentes militares y civiles siendo estos últimos los dominantes.

Para Darczewska[7] "en la doctrina rusa, no se encuentra ninguna idea con respecto del uso del ciberespacio en los conflictos armados para destrucción de recursos de información del enemigo". Esta afirmación no permite interpretar el espíritu ruso a la luz de los hechos acontecidos en Ucrania, donde es posible apreciar que la población fue afectada de forma reiterada siendo privada del uso de servicios esenciales dependientes de la matriz eléctrica; o bien en caso Estonia 2007 donde también los ciudadanos de Tallin fueron el blanco de ciberoperaciones a través de la afectación de infraestructura critica y la denegación de servicios como transporte y servicios bancarios originándose una situación de caos social durante el termino de un mes.

Existen otras visiones donde se considera que los métodos rusos actuales son mucho más avanzados que los que se emplearon contra Georgia en 2008, particularmente a través de redes sociales con objetivos específicos, citando la publicación "Social Media as a Tool of Hybrid Warfare" del Centro de Comunicaciones Estratégicas de la OTAN donde se señala la existencia de troles híbridos que operan en el contexto de una determinada agenda militar o política (Collins, 2018)

[7] Darczewska, Jolanta, "The devil is in the details: Information Warfare in the light of Russia's Military Doctrine, Point of View, Number 50,
Warsaw, May 2015, Disponible en: https://www.osw.waw.pl/sites/default/files/pw_50_ang_the-devil-is-in_net.pdf

En un reconocido artículo publicado en la revista Military Review, el General ruso Valery Gerasimov sostuvo *"*que los medios no militares se utilizan cuatro veces más a menudo en los conflictos modernos que las medidas militares convencionales".

Según de Vergara y Trama (2017), esto se vio reflejado en Crimea en el año 2014, "*cuya anexión se basó en gran medida en el empleo sobre todo de fuerzas especiales*" y que "*el uso de estas tropas de élite, junto con una campaña de guerra de la información y el despliegue de grupos que tienen una amplia simpatía con los objetivos de Rusia (servidores proxies), creó las circunstancias que sentaron las bases para una adquisición convencional, sin derramamiento de sangre, logrando frenar el proceso de integración con Europa occidental".*

Se reafirma en estos conceptos, otra faceta de empleo del ciberespacio anteriormente mencionado, para la guerra de la información sincronizada con el accionar de medios no convencionales teniendo como objetivo la población local y su percepción del entorno.

Respecto a la dimensión tiempo; las acciones se iniciaron desde la paz, sin pasar por las escalas tradicionales de un conflicto – tensión, crisis, guerra-. Y respecto a la dimensión espacio, nuevamente vemos lo restrictivo de considerar de forma taxativa el concepto doctrinario de Teatro de Operaciones.

De Vergara y Trama citan que "las operaciones cibernéticos no son planificadas desde que se decide el empleo de las Fuerzas Armadas, sino que se inician desde que se anticipa la contingencia en el planeamiento de la estrategia militar". En tal sentido, se aprecia una concordancia con los hechos acontecidos en Crimea, lo cual permite inferir de la sincronización con Operaciones de Información y el empleo de Fuerzas Especiales, en pos de lograr la alteración de las condiciones del Ambiente Operacional en oportunidad con un grado de secuencialidad que responde a una intencionalidad manifiesta.

También describen que "las opciones cibernéticas, comprenden medidas defensivas, ofensivas y exploratorias". Se considera que estas últimas, por su naturaleza requieren su aplicación de forma previa al empleo de las FFAA.

Conclusiones Parciales

En función de los contenidos abordados durante el primer capítulo, se considera que;

- El marco legal existente en nuestro país, que separa Defensa y Seguridad Interior, y del mismo modo con la actividad de Inteligencia, dificultan la articulación de una respuesta eficiente en oportunidad para hacer frente a amenazas hibridas que puedan constituirse que valiéndose del espacio cibernético pueden desarrollar capacidades que afecten la infraestructura critica del país y por consiguiente a la población; no solo en la vida diaria sino también en la percepción del contexto.
- El establecimiento de un Teatro de Operaciones como un aspecto doctrinario poco flexible, la escaza integración interagencial, y el limitado intercambio de información entre el sector privado (poseedor de la mayor parte de la infraestructura critica del país) y agencias estatales, impiden hacer frente de manera eficiente a efectos generados a través del espacio cibernético afectando el status quo en las condiciones del Ambiente Operacional.
- La imposibilidad de identificar de forma certera la autoría de los efectos que se producen haciendo uso del ciberespacio, dificultan el trabajo interagencial para canalizar de manera oportuna las actividades y tareas necesarias para preservar la prestación de servicios esenciales particularmente en grandes urbes.
- Todos los aspectos anteriormente señalados, dificultan la protección de los Objetivos de Valor Estratégico, hoy en día estarían bajo la responsabilidad del Sistema de la Defensa, y cuya afectación tiene un impacto significativo en la conducción de las operaciones militares en todos los niveles.
- La limitación que existe para el campo de la Inteligencia Militar dada por el marco legal y el doctrinario para el nivel operacional, dificultan la anticipación frente a la constitución de potenciales amenazas cibernéticas cualquiera sea su origen.
- La ausencia de políticas nacionales particulares para el uso del ciberespacio, impacta por consiguiente en el nivel operacional limitando el desarrollo y ejecución de capacidades ofensivas y de exploración ante la certeza de la constitución de una contingencia producto de una amenaza cibernética.
- La existencia de un Comando Conjunto de Ciberdefensa que se encuentra en los prolegómenos de su capacidad doctrinaria, operativa y de integración al esfuerzo

de la Defensa puede verse limitado por un marco legal que responde a parámetros tradicionales, para el desarrollo y empleo de capacidades ofensivas y exploratorias ante potenciales amenazas que se constituyan en el ambiente cibernético.

Capítulo II: El impacto de las Ciberoperaciones sobre las condiciones del Ambiente Operacional

El presente capítulo está centrado en el impacto de las Ciberoperaciones sobre las condiciones del Ambiente Operacional, a la luz de casos de relevancia a nivel mundial.

El Ambiente Operacional y sus implicancias.

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"; La doctrina conjunta, agrega lo factores políticos, económicos y sociales.

El Ambiente Operacional, requiere de un análisis sistémico en cuanto a su composición, y está integrado por una serie de factores interrelacionados, lo cual implica el análisis de la información disponible desde múltiples perspectivas, en pos de una visión más amplia y objetiva.

Para Christopher S. Chivvis[8] "*Capturar el territorio sin tener que recurrir a la fuerza militar abierta o convencional fue el objetivo de la exitosa anexión de Crimea a Rusia en el año 2014, una jugada que puso en marcha el debate sobre las "estrategias híbridas" rusas. La anexión de Crimea se basó en gran medida en el empleo sobre todo de fuerzas especiales que operaron a través de un comando de operaciones especiales ruso recién creado. El uso de estas tropas de élite, junto con una campaña de guerra de la información y el despliegue de grupos que tienen una amplia simpatía con los objetivos de Rusia (proxies), creó las circunstancias que sentaron las bases para una adquisición convencional, sin derramamiento de sangre, de Crimea."*

Se reafirma con los contenidos desarrollados, que el principal objetivo estaba dado por la población, siendo la variable más de relevante en los conflictos híbridos. Para la doctrina argentina, es una variable dentro de los factores del Ambiente Operacional.

Los casos que a continuación se describen, evidencian como podría verse alterado el status quo del Ambiente Operacional en contextos diferentes pero teniendo como uno de los actores a Rusia haciendo el uso del ciberespacio como estado o a través de terceros actores no estatales.

---

[8] Chivvis, Christopher S. Testimony of The RAND Corporation Understanding Russian "Hybrid Warfare" and What Can be Done About It.
Disponible en:
http://www.rand.org/content/dam/rand/pubs/testimonies/CT400/CT468/RAND_CT468.pdf

El caso Estonia (2007)

El caso de Estonia, es considerado el primer ciberataque a gran escala**.** Para 2007 el país era un referente global por su alto grado de conectividad y no existía situación de conflicto alguno en el marco externo como así tampoco en el marco interno con las minorías rusas que viven en el país desde la era soviética.

En Tallin la ciudad capital, se encuentra un monumento al soldado ruso de la Segunda Guerra Mundial que conmemora la liberación de la ocupación alemana, el cual ha sido punto de encuentro cada vez que los ruso-estonios han efectuado manifestaciones contra las autoridades. En 2007 el gobierno decidió retirar la estatua del emplazamiento para colocarla en un sitio menos central, como venía sucediendo en los tres países bálticos con los símbolos de la era comunista soviética.

La respuesta de los ruso-estonios se materializó el 27 de abril de 2007, en la forma de protestas que escalaron en saqueos y destrucción de propiedades públicas y privadas; todas las demostraciones fueron contenidas y en el transcurso de una semana todos los daños físicos estuvieron reparados (AFCEA International, 2012).

Cuando el conflicto físico hubo terminado, los sitios de la administración de gobierno, los de los bancos y muchos otros sitios de noticias y servicios web fueron sistemáticamente afectados mediante ataques de denegación de servicio (Sepetich, 2016)

Estos ataques iniciaron el 27 de abril y se extendieron por espacio de tres semanas. Durante ese lapso distintos servicios como páginas gubernamentales, sistemas bancarios, agencias de noticias y sitios de comercio electrónico estuvieron inoperativos (Richards, 2016).

En este caso, los actores que se vieron involucrados fueron el Gobierno de Estonia, como principal y otros secundarios constituidos por actores privados de ese país, diarios, asociaciones técnicas, hacktivistas[9] e individuos de la población.

En contraposición, hacktivistas rusos y rusos-estonianos y presuntamente, según distintas fuentes, podrían haber contado con el apoyo de organismos del gobierno ruso, lo cual no ha sido probado.

Como tercer parte, tomarían intervención la OTAN y aliados públicos y privados de Finlandia, Israel y Eslovenia.

Los efectos inmediatos, fueron la pérdida de control de más del 90% de servicios esenciales y comerciales, afectación total del sistema de transporte ferroviario del país;

[9] Hacktivista; individuo que se vale de medios informáticos para la realización de agitación política

la provocación del caos digital dada la alta dependencia del país de la tecnología y conectividad. De esta forma, se generó caos entre la población de Tallin, privada de servicios esenciales alcanzando una situación de emergencia nacional de forma súbita que se sostuvo por un mes.

En respuesta al impacto de los hechos, la OTAN y Unión Europea, crearon en Estonia el Centro Cooperativo de Ciberdefensa de Excelencia, y la Agencia Europea estableciendo estrategias defensivas sobre sistemas de información tecnológica a gran escala.

El caso Ucrania. La Guerra Hibrida

"*Hasta no hace mucho tiempo atrás, y en algunos países aún lo siguen siendo, las operaciones cibernéticas y las operaciones con fuerzas especiales eran consideradas como complementarias a las tradicionales y, por lo tanto, tomadas en consideración después de que se formulan los planes esquemáticos. Sin embargo, en el caso de la guerra entre Rusia y Georgia en 2008 y entre Rusia y Ucrania en 2014, las fuerzas convencionales fueron dejadas como operación complementaria en un papel disuasorio y como parte de un plan de engaño, en tanto que las operaciones cibernéticas y las fuerzas especiales tuvieron la prioridad de las operaciones militares*" (Trama, 2017)

La afectación de la población, puede cambiar la percepción sobre un conflicto y la relación con el gobierno de un país. La guerra hibrida llevada adelante por Rusia contra Ucrania da claras muestras de la transformación de ello, y la certeza de que estas son articuladas con operaciones de información, y el empleo de Fuerzas Especiales para potenciar los efectos, como ocurrió en Crimea.

Para De Vergara y Trama, las Operaciones Cibernéticas en Ucrania, se constituyeron como las principales; y menciona que "*el Ministerio de Defensa de Ucrania debió emigrar a otro país para poder dirigirse a sus fuerzas, ya que su acceso a los medios de comunicación ucranianos le estaba técnicamente vedado*." Esto permite dimensionar el alcance, donde la estrategia militar, se ve alcanzada e imposibilitada de ejercer las actividades básicas como el comando, el control y la comunicación.

La afectación de infraestructura critica sensible, se vio de manera reiterada en Ucrania. La alteración intencional del servicio eléctrico en 2016 utilizando el troyano Blackenergy en la región ucraniana de Ivano-Frankovsk afectó a un número de 1,5 millones de habitantes). De modo similar, en 2017, se producen otros incidente a través del ciberespacio con consecuencias físicas, afectando en este caso el nivel de

transmisión en una subestación, cuya función es la de establecer niveles de tensión adecuados.

Las consecuencias sistémicas de la afectación del sistema de energía, son múltiples y de lo más variadas en cuanto a su alcance, pero con la certeza de la afectación del normal funcionamiento de los servicios esenciales para la vida diaria especialmente en las grandes urbes.

La denegación de servicios, como la telefonía celular y servidores de la red bancaria, también fueron corrientes en Ucrania.

La telefonía celular, amerita una mención aparte. "*El Gobierno ruso ha hecho todo lo posible para controlar la información pública sobre la actividad de sus tropas en Ucrania. Nadie, sin embargo, ha desafiado tanto el monopolio de la inteligencia militar del Kremlin como sus propios soldados, que como la mayoría de los jóvenes en Rusia, son ávidos usuarios de las redes sociales. Ya sea por los bombardeos encubiertos a objetivos dentro de Ucrania o incluso las incursiones secretas dentro de ese territorio, los soldados rusos han accionado repetidamente la opción "eliminar mensaje" luego de haber difundido evidencia de las intervenciones ilegales o, lo que es peor, no habiendo publicado absolutamente nada, lo que sugiere que fueron capturados o muertos en combate.*

A pesar de que las reglas lo prohibían, muchos soldados rusos llevaron al frente teléfonos celulares con conexión a internet, que luego utilizaron para actualizar sus cuentas en Vkontakte, la red social más popular de Rusia." (Global Voices; 2017)

Se aprecia la vulnerabilidad de las MSCI (Medidas de Seguridad de Contrainteligencia), al tiempo que el normal funcionamiento facilita el desarrollo de Operaciones de Información sobre la población.

Para De Vergara y Trama "*Del mismo modo, cada vez más dispositivos de comunicación, por ejemplo, celulares, los teléfonos inteligentes, son capaces de transmitir y recibir información de voz y datos, haciendo más difusas las líneas que tradicionalmente separaban los campos de la conducción entre inteligencia, operaciones y comunicaciones. Esto ha llevado a la integración de las operaciones cibernéticas a la Guerra electrónica, a las operaciones de inteligencia, a las operaciones en el espectro electromagnético ya las operaciones de información."*

De los conceptos señalados, se aprecia, que el desarrollo de operaciones cibernéticas que afecten las condiciones del Ambiente Operacional, debe estar sincronizado y coor-

dinado con Operaciones de Información, Inteligencia, Guerra Electrónica, el accionar de Fuerzas Especiales, y de la no conveniencia respecto a la generación de efectos de forma aislada, a fin de no alterar las condiciones de forma tal que pudieran ser contra-producentes para la propia conducción de las operaciones militares en desarrollo.

Conclusiones parciales

De los aspectos abordados en el Capítulo 2 del presente TFI, se visualiza que;

- Las Operaciones cibernéticas, tienen la capacidad de alterar las condiciones del Ambiente Operacional y la percepción de la sociedad. El alcance de los efectos tiene un carácter sistémico y puede alcanzar el estado de caos para la población de grandes urbes de manera proporcional al grado de desarrollo de la conectividad que la región posea.
- Las operaciones que se realicen para mantener el status quo o bien modificar las condiciones del Ambiente Operacional, requieren ser preparadas, coordinadas, y sincronizadas con otro tipo de operaciones, como las de Información, estableciendo de forma clara la oportunidad, secuencia y prioridades a fin de lograr los efectos perseguidos.
- Dichas operaciones no pueden ser ejecutadas de forma aislada por los efectos colaterales que generan, cuyo alcance es difícilmente estimable sin un profundo grado de conocimiento de todas las variables plausibles de ser alcanzadas y que deben responder a un proceso de planeamiento lógico en concordancia con el diseño operacional, la intención del Comandante y las limitaciones impuestas.
- La afectación de la percepción de la población no se limita a los medios medios de comunicación masiva tradicionales, sino que encuentra en las aplicaciones sociales una nueva forma concordante con las prácticas habituales de los habitantes de una región.
- La protección de la infraestructura critica y la integracion interagencial, requieren ser abordadas desde las más altas esferas de la estrategia nacional estableciendo políticas, lo que excede al nivel operacional.
- Dentro de la infraestructura critica, aquella que afecte a los Medios de Comunicación Social, y las Telecomunicaciones, requieren una atención particular a fin de disponer de las prestaciones necesarias para explotar estos medios a favor en el desarrollo de las Operaciones de Información.

Capítulo III: Tendencias doctrinarias contemporáneas para el empleo militar del ciberespacio

Para el desarrollo de este capítulo, fueron seleccionados tres países; Rusia, Lituania y Estados Unidos de América.

El primer caso, responde a su participación en conflictos recientes bajo el marco conceptual de lo que Occidente denomina "Doctrina Gerasimov", donde la incidencia del empleo del ciberespacio para modificar las acciones del Ambiente Operacional, ha sido significativa y de un alto impacto, a la luz de los hechos sucedidos en Ucrania.

El segundo caso se corresponde con la República de Lituania, por su ubicación geográfica, antecedentes sociales, políticos, económicos e históricos (buscando una analogía con el caso Estonia de 2007), para visualizar como aborda un país pequeño la problemática que se deriva de enfrentar un escenario hipotético del empleo del ciberespacio.

El tercer caso, se corresponde con los Estados Unidos de América, por ser un actor global con capacidad de cambiar las reglas de juego en cualquier escenario, razón por la cual aborda la problemática de forma integral, desarrollando capacidades ofensivas, defensivas y exploratorias.

La sensibilidad del tipo de información, dificulta la obtención de contenidos que se centren en el nivel de interés a través de fuentes abiertas. No obstante, se busca resaltar los aspectos particulares que sean de utilidad para el establecimiento de conclusiones parciales en pos de los objetivos específicos del presente capítulo sobre la base de los documentos a los que se ha accedido.

Rusia

Rusia es un referente en el empleo militar del ciberespacio a nivel global. En Occidente, se habla de "Doctrina Gerasimov", para describir el carácter evolutivo de cómo Rusia hace la guerra en los conflictos recientes en lo que ha tomado parte de forma directa o indirecta, y donde el desarrollo de ciberoperaciones constituye un brazo importante.

No es posible acceder su doctrina a través de fuentes abiertas o de otro tipo. Es por ello que numerosos analistas militares especializados en Rusia han buscado abordar tres textos militares que han sido foco de atención en los últimos años.

Se busca a través de ello, dar una interpretación lógica que permita arribar a conclusiones objetivas respecto a la concepción en dicho país, en el desarrollo de conflictos, para visualizar aspectos de interés para el presente TFI.

La revista de la Academia de Ciencias Militares de Rusia, transcribió y publicó el discurso del General Valery Gerasimov, Jefe del Estado Mayor General. En dicha publicación se identifican a través de sus afirmaciones, ciertas tendencias que se resumen de la siguiente manera;

- Las guerras en la actualidad no se declaran
- Las revoluciones de los colores (demostraciones populares organizadas para socavar instituciones gubernamentales) pueden ocurrir de forma rápida
- Las guerras de nuevo tipo (no utiliza el término guerras hibridas, propio del mundo occidental) son como las guerras regulares.
- Los métodos no militares en ocasiones son más efectivos que los métodos militares. (Gerasimov, 2013)

Asimismo afirma que "algunas naciones emplean una combinación de métodos no militares, entre ellos el potencial de las manifestaciones populares, las medidas militares encubiertas y las actividades de las fuerzas especiales, para controlar los conflictos", aspectos que se considera pudieron ser observados en el conflicto de Ucrania en la región de Crimea a partir de 2014.

Luego enumera una serie de cambios, que a los fines de esta investigación, se seleccionan los que son de interés sobre cómo se lleva a cabo una guerra contemporánea; donde manifiesta que el más relevante pasa por evitar el contacto, enfrentando al oponente de forma remota – reducción del tiempo y espacio; luego habla de un equilibrio entre los niveles de la guerra. En ambos casos facilitado por el empleo de la tecnología.(Gerasimov, 2013)

Para Thomas (2017) en un artículo de Military Review de Octubre de 2017 que analiza dicho texto y los de otros mandos rusos cita que "*la descripción de formas y métodos es seguida por una evaluación sobre cómo mejorar el concepto de defensa territorial" y luego sostiene que "todo indica que durante el ejercicio Kavkaz 216, el Centro Nacional de Gestión de Defensa ruso, cumplió con el objetivo de mejorar la defensa del territorio nacional al encargarse de la integración de estructuras militares y civiles*".

De un segundo texto correspondiente al Coronel Chekinov, publicado en la revista Pensamiento Militar en 2013, se destaca una afirmación indicando que "*la superioridad informativa y las operaciones de anticipación serán los ingredientes principales que permitirán el éxito en las guerras de la nueva generación*".(Chenikov, 2013)

Respecto de estos artículos, Thomas (2017) cita en relación con dicha conclusión que "*ningún objetivo se alcanzara en las guerras futuras a menos que un beligerante gane la superioridad informativa sobre el otro*". Cuando se refiere a superioridad informativa, cita que se refiere "*a la presión informativa que se puede ejercer a través de los medios de comunicación, organizaciones no gubernamentales, subvenciones extranjeras, organizaciones religiosas, propagandas y desinformación designados para alimentar el caos en la sociedad*"

Del tercer artículo, de la revista de la Academia de Ciencias Militares de Rusia, Thomas considera que el aspecto más importante es "que nuevos y mejorados recursos y métodos para llevar a cabo conflictos militares contemporáneos están en aumento y sin capaces de generar nuevas formas de conflicto también" (Kartapolov, 2015)

El nivel operacional ruso contempla una visión más amplia de la guerra, más allá del mero empleo militar, donde incorpora organizaciones no gubernamentales, el manejo de los medios de comunicación, sanciones económicas, acciones diplomáticas y presiones políticas, dentro de un tablero internacional, cada vez más globalizado y complejo (Bartles, 2016)

OTAN- República de Lituania

El Libro Blanco de la Defensa de Lituania establece que el sistema de defensa del país está basado en el concepto de "defensa integral e incondicional" derivada de la Estrategia de Seguridad Nacional. El objetivo de la política de defensa de Lituania es preparar a su sociedad para la defensa general e integrar Lituania en las estructuras de seguridad y defensa occidentales, en clara referencia a la Organización del Tratado del Atlántico Norte (OTAN), de la cual este país es miembro.

Posee una Ley de Ciberseguridad promulgada en el año 2014, que articula los componentes del Estado en pos de los objetivos dictados por la política desde el nivel estratégico. El Ministerio de Defensa, entiende en lo referente a la Ciberseguridad, e integra el sistema interagencial a través del "Nacionalinis Kibernetinio Saugumo Centras" (Centro Nacional de Seguridad Cibernética) integrado también por el Gobierno, el Ministro del Interior, la Autoridad Reguladora de las Comunicaciones, la

Inspección Estatal de Protección de Datos, el Departamento de Policía. Existe un Consejo, encabezado por el Ministerio de Defensa.

Del análisis de las distintas partes de la ley, se observa que;

- Se aborda una visión integral, interagencial y dinámica, lineamientos claros en cuanto a responsabilidades y el intercambio de información.
- La relevancia que se le otorga a la infraestructura critica, en particular aquella relacionada con los servicios esenciales para la población donde sobresale la red eléctrica.
- Las competencias que se le otorgan a los entes del estado que entienden para accionar ante casos de necesidad (ciberataques) en pos del bien común y sin intervención de la justicia por un periodo de 48 horas.
- La divulgación de información de interés a la población, cuando desde el punto de vista de la Ciberseguridad se detecten potenciales amenazas tales como la preservación de la información personal.
- Dicho centro interagencial, se ocupa de los redes de organismos públicos, pero que dicta pautas para el cumplimiento por parte del sector privado, y que no obstante este es responsable de su propia seguridad informática, siempre y cuando no esté relacionado con el sector energético o gestión de instalaciones que se cataloguen como infraestructura critica. (Presidencia de la República de Lituania, 2014)

De la forma en que este país encara los desafíos que plantea el uso del ciberespacio, y si situación particular por la cual fue seleccionado, se considera de particular interés, la concepción del trabajo interagencial entre los órganos del estado, la importancia que se le asigna a protección de la matriz energética y la diseminación de la información de interés para la población, como variable más susceptible de lo que a la luz de nuestra doctrina consideramos el Ambiente Operacional.

Asimismo, la existencia de políticas emanadas desde el nivel estratégico, permite establecer lineamientos claros para los componentes que entienden, participan e intervienen en la gestión de redes e infraestructura critica. Y que el esfuerzo en pos de mantener el status quo de las condiciones del Ambiente Operacional de interes para el nivel de estudio del presente TFI, es la resultante de la confluencia de las actividades y tareas de competencia de las distintas agencias del estado, de forma integral y sinérgica

a diferencia de nuestra visión compartimentada producto de un marco legal restrictivo para hacer frente a nuevos paradigmas.

Estados Unidos de América

El Departamento de Defensa de EEUU, presento en el año 2015, la nueva Estrategia de Ciberseguridad del Pentágono, "The DoD Cyber Strategy" (DoD) señalando los objetivos a lograr en materia cibernética por el Departamento de Defensa hasta el año 2018. Allí se plantean actividades de ciberguerra afirmando que los EEUU, "deben ser capaces de recurrir a las ciberoperaciones para destruir las redes de mando y control, infraestructuras críticas o sistemas de armas de los potenciales adversarios del país".

Cuando se refiere a potenciales adversarios, lo entiende no solo como Estados, sino también como organizaciones no estatales. Asimismo, se aprecia que hasta la implementación del DoD, se hace referencia en dicho país, al término Ciberdefensa. Así lo vemos reflejado en la denominación en el caso del componente terrestre; "US Army Cyber Command (ARCYBER).

El DoD, da lineamientos, entre los cuales cabe destacar;

- La necesidad de incrementar la cooperación entre actores estatales, privadas y aliados de dicho país.
- Utilización de capacidades de manera ofensiva, no limitándose a la naturaleza pasiva de la Ciberdefensa, ni la explotación de ataques derivada de dicha actividad.
- La no consideración de la OTAN, como un actor en la materia

Asimismo, se considera de importancia subrayar tres aspectos que se mencionan en dicho documento como misiones primarias para el Departamento de Defensa de EEUU en materia de Ciberoperaciones.

- La primera, la defensa de sus redes, sistemas e información
- La segunda, estar preparado para defender a los EEUU y sus intereses, de ciber ataques de consecuencias significativas
- La tercera, estar en capacidad de proporcionar ciber capacidades integradas para apoyar operaciones militares y planes de contingencia

En función de lo que se considera esencial extraer en cuanto al contenido de ese documento, para establecer cuál es el estado del arte, y las posibles tendencias de un actor de relevancia a nivel mundial, podemos señalar que se evidencia la necesidad de hacer frente a amenazas que no están circunscriptas a actores tradicionales; que el

ámbito del ciberespacio, no solo es un dimensión más para la lucha de voluntades, sino también un medio, para a través de este, lograr daños físicos sobre la infraestructura critica de uno de los actores. Y que la naturaleza de la actividad, no renuncia a la esencia misma, que es la protección de la información y los propios sistemas, pero que no se desconoce la necesidad de contar con las capacidades que permitan mantener la iniciativa, lo cual implica la toma de una postura ofensiva en el ciberespacio.

Un aspecto no menor, que se desprende de ello, es la dimensión tiempo; porque las mismas acciones que podrían ser necesarias en tiempo de guerra, también pueden llegar a serlo en tiempo de paz, en pos de configurar situaciones favorables para una de las partes. Esto implica el uso de medidas exploratorias.

Por otro lado, la necesidad que plantea dicho documento, de una integración con actores privados siendo estos los operadores de la mayor parte de la infraestructura critica.

Conclusiones Parciales

Como conclusiones parciales de este capítulo, se señala que;

- Los principales actores a nivel global desarrollan capacidades ofensivas, defensivas y exploratorias y que estas últimas se ejecutan desde la paz o la detección de una contingencia potencial.
- Las capacidades defensivas constituyen en centro de gravedad propio desde el punto de vista de la ciberfedensa, para asegurar el Comando y Control por parte del Instrumento Militar en el nivel operacional.
- Las capacidades ofensivas y exploratorias, son las que permiten alcanzar la infraestructura critica cuya afectación transforma las condiciones del Ambiente Operacional, siendo la población la variable más sensible.
- Para enfrentar un escenario hibrido se requiere de una concepción dinámica, considerándose la integración interagencial la más eficiente. La determinación de autoria pierde relevancia de forma inicial, primando la protección de la infraestructura critica sensible y la percepción de la sociedad.
- Se requieren criterios emanados desde el más alto nivel para facilitar la interacción con el sector privado y la adopción de criterios comunes que permitan estandarizar procedimientos comunes.
- El marco legal es fundamental para establecer una concordancia entre los niveles estratégico, operacional y táctico; y que el nivel de interés, no está en capacidad de suplir con el desarrollo de capacidades, los vacíos que existan desde la estrategia nacional para la integración de componentes, o el direccionamiento eficiente para el empleo del instrumento militar.
-

Conclusiones Finales

Las operaciones en el ciberespacio, responden a una acepción multidisciplinar que abarca todos los factores de poder nacional y requiere la aplicación de políticas de Estado que los guíen y orienten, siendo el militar sólo uno de ellos. En función de ello, se considera que;

- El marco legal vigente en la República Argentina, que separa Defensa y Seguridad, y limita al campo de la Inteligencia militar, no es adecuado para hacer frente a los nuevos paradigmas que plantea la aparición de un nuevo dominio. Este aspecto de base tiene repercusiones en todos los niveles para la concepción, planificación, desarrollo y ejecución de actividades y tareas que responden a la necesidad militar para la conducción de operaciones desde el Nivel Operacional. Asimismo dificulta el abordaje de la problemática de forma integral y sinérgica al limitar otras actividades necesarias como las Operaciones de Información, y el intercambio de información con el sector privado, poseedor del grueso de la infraestructura critica sensible.
- A consecuencia del marco legal vigente, prevalece una visión compartimentada sobre cómo hacer frente a las amenazas cibernéticas, dificultando dar respuestas oportunas y eficientes a la luz de la evolución de estado del arte que se refleja en casos de relevancia a nivel mundial, donde las condiciones del Ambiente Operacional se vieron afectadas en rápidas escaladas, sin que existiera una situación de tensión o crisis, con consecuencias sistémicas sobre el normal desarrollo de la vida diaria en una sociedad que van más allá de las operaciones militares propiamente dichas
- La imposibilidad de desarrollar capacidades ofensivas y exploratorias, impiden dar respuestas que permitan neutralizar de manera preventiva o preemptivas a amenazas cibernéticas que se consoliden y con capacidad de afectar servicios esenciales para la población.
- Los aspectos doctrinarios que implican la constitución de un Teatro de Operaciones, limitan el empleo de medios cibernéticos en tiempo y espacio, considerándose un aspecto incongruente y anacrónico para hacer frente a las

amenazas cibernéticas que posean la capacidad de afectar las condiciones del Ambiente Operacional.

- Las capacidades necesarias para emplear en el ciberespacio a fin de preservar o modificar las condiciones del Ambiente Operacional son las defensivas, ofensivas y exploratorias, y que estas tienen un valor polivalente para el desarrollo de Operaciones de Información, para la reducción de interferencia a la población (o bien su empleo a favor), el apoyo a las operaciones desarrolladas por las fuerzas especiales y la sincronización de efectos.
- La concepción interagencial es la más adecuada para hacer frente a amenazas cibernéticas que pudieran afectar infraestructura critica del país, como así también desarrollar Operaciones de Información o hacer cualquier otro uso del espacio cibernético que pudieran afectar el status quo, y que la adecuación del marco regulatorio, escapa al Nivel Operacional.
- La protección de infraestructura crítica sensible es una problemática de relevancia para el Nivel Operacional en pos de una eficiente conducción de las operaciones, y que requiere de un intercambio fluido con el sector privado, poseedor de la mayor parte. No obstante es una problemática que escapa al nivel de interés.
- La afectación sistémica de servicios esenciales, impacta directamente en la conducción de operaciones militares, donde la población es la variable más vulnerable en el marco de la Guerra Hibrida, y que la generación de efectos a través del ciberespacio, se complementa con Operaciones de Información, Inteligencia y el empleo de Fuerzas Especiales, pudiendo en el Nivel Operacional, alterar forma súbita la prioridad de empleo de medios frente a las necesidades de la población.
- En virtud de las conclusiones a las que se ha arribado en el presente TFI, se aprecia que es necesario ampliar la visión actual sobre la Ciberdefensa, y que esta problemática no puede ser emanada desde el Nivel Operacional. La Adecuación o particularización del marco legal se considera la piedra fundamental para hacer frente a los nuevos desafíos que plantea la aparición de un quinto dominio que atraviesa los anteriormente conocidos, y que como consecuencia de ello, requiere de una visión integral de la problemática planteada.

- Como corolario final, considerando que la quinta dimensión requiere de una visión multifacética que no es congruente con la visión tradicional de los conflictos; que tiene implicancias multi jurisdiccionales, sobre el sector civil, militar; acciones tácticas, pueden tener efectos estratégicos a un bajo costo; el alcance de los efectos, puede ser de distinto grado, y puede escapar a la intención del planeamiento, trayendo aparejadas consecuencias colaterales imprevistas; el anonimato dificulta establecer el propósito de las intrusiones en las redes cibernéticas; es por ello que se considera que las actividades en el ciberespacio requieren de un esfuerzo que englobe en su conjunto a múltiples agencias del estado, sin límites rígidos para dar respuestas adecuadas y oportunas; que las operaciones cibernéticas tienen dos matrices; una relacionada a efectos sobre objetivos y otra sobre el desarrollo de operaciones de información e inteligencia; que su empleo es pleno y conveniente desde la detección de una potencial contingencia; que los principios de la guerra no son de plena aplicación al quinto dominio; que la planificación hoy se ve totalmente limitada a parámetros tradicionales para hacer frente a una realidad del siglo XXI; que la velocidad con la que se sucintan los incidentes en el ciberespacio, y la vulnerabilidad del sector civil que opera infraestructura critica sensible; hacen necesario el establecimiento de un marco legal particular para hacer frente a esta problemática, adecuado a esta nueva realidad con políticas que se establezcan desde el nivel estratégico e impacten en el operacional y táctico; buscando una concepción interagencial flexible y mancomunada, que derive en la adecuación de la doctrina conjunta, en particular para no limitar las acciones a la dimensión tiempo y espacio de un Teatro de Operaciones, y permita el pleno empleo de capacidades para dar respuestas eficientes y acordes a esta nueva realidad.

Bibliografía

- AFCEA International. (2012). "*The Russo-Georgian War 2008: The Role of the Cyber Attacks in the Conflict".* AFCEA International.

- Bartles, C. (2016). "*Como comprender el articulo de Gerasimov". Military Review* , 55-63.

- Calvo,Carvalho, Paulo Sergio, *Defesa Cibernética e as Infraestruturas Críticas Nacionais, Anais Do X Ciclo De Estudos Estratégicos*: Proteção Das Infraestruturas Críticas, Disponible en: http://www.eceme.ensino.eb.br/meiramattos/index.php/RMM/issue/view/15

- Collins, D. (2018). Military Review. *Los métodos y las acciones de Rusia contra EEUU y la OTAN*. Recogido de www.armyupress.army.mil

- Casar Corredera, José Ramón, "*El Espacio cibernético: Nuevo escenario de confrontación*", Centro Superior de Estudios de la Defensa Nacional, Monografías del CESEDEN, febrero de 2012, P. 14; Disponible en; :http://www.defensa.gob.es/ceseden/Galerias/destacados/publicaciones/monografias/ficheros/126_EL_ESPACIO CIBERNÉ-CO_NUEVO_ESCENARIO_DE_CONFRONTACION.pdf

- Cicerchia, C. (2017). Ciberdefensa. *Seminario de Ciberdefensa*. Exposición llevada a cabo en la ESG, Buenos Aires.

- Chenikov, G. (2013). *On the character and content of wars of a new generation.* Revista Pensamiento Militar

- Chivvis, Christopher S. "*Testimony of The RAND Corporation Understanding Russian "Hybrid Warfare" and What Can be Done About It*."

- Disponible en: http://www.rand.org/content/dam/rand/pubs/testimonies/CT400/CT468/RAND_CT468.pdf

- Darczewska, Jolanta, "*The devil is in the details: Information Warfare in the light of Russia's Military Doctrine, Point of View"*, Number 50, Warsaw, May 2015, Disponible en: https://www.osw.waw.pl/sites/default/files/pw_50_ang_the-devil-is-in_net.pdf

- Departamento de Defensa de los Estados Unidos de América (2015). *Directiva de Ciberestrategia.* Recuperado de www.defense.gov

- De Vergara, E. y Trama, G. "*Operaciones militares cibernéticas: Planeamiento y Ejecución en el Nivel Operacional*." Buenos Aires: Escuela Superior de Guerra Conjunta de las Fuerzas Armadas.

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

- Escuela Superior de Guerra del Ejército. (1993). *Bases para el Pensamiento Estrategico, Estrategia Operacional.* Buenos Aires: Escuela Superior de Guerra del Ejército "Tte Grl L M Campos".

- Gerasimov, V. (2013). *Principal trends in development of forms and methods of employing Armed Forces and current tasks of military science regarding their improvement.* Revista de la Academia de Ciencias Militares de Rusia.

- Global Voices (2014). "*Para los soldados rusos el telefono celular podria sertan poderoso como una espada"*. Recuperado de www.globalvoices.org

- Guimpel, L. (2018). Ciberdefensa. *Ciberdefensa*. Exposición llevada a cabo en el CCCD, Buenos Aires

- Honorable Congreso de la Nación. (1988). *Ley de Defensa Nacional Nro 23.554.* Recuperado de www.infoleg.com.gob.ar

- Honorable Congreso de la Nación. (1992). *Ley de Seguridad Interior Nro 24.059.* Recuperado de www.infoleg.com.gob.ar

- Honorable Congreso de la Nación. (1992). *Ley de Inteligencia Nacional Nro 25.520.* Recuperado de www.infoleg.com.gob.ar

- Joint Publication (JP) 1-02, Department of Defense Dictionary of Military and Associated Terms.

- Kartapolov, A. (2015). *Lessons of military conflcits and prospects for the development of resources and methods of conducting them. Direct and indirect actions in contemporary international conflicts*. Revista de la Ademia de Ciencias Militares de Rusia.

- Mando Conjunto de Ciberdefensa de España (2018). *Funciones*. Recuperado de www.defensa.gob.es

- Ministerio de Defensa de Argentina. (2015). *Manual de Estrategia y Planeamiento para la Acción Militar Conjunta, Nivel Operacional, La Campaña, MC 20-01* . Buenos Aires: Ministerio de Defensa de Argentina

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

- Ministerio de Defensa de Argentina. (2015). *Libro Blanco de la Defensa.* Buenos Aires: Ministerio de Defensa de Argentina.

- Ministerio de Defensa de Argentina. (2015). *Planeamiento para la Acción Militar Conjunta, Nivel Operacional, PC 20-01*. Buenos Aires: Ministerio de Defensa de Argentina.

- Ministerio de Defensa de Lituania. (2015). *Libro Blanco de la Defensa.* Vilnius: Ministerio de Defensa de Argentina.

- Poder Ejecutivo Nacional. (2018). Decreto 703/18. *Directiva Politica de Defensa Nacional*. Recuperado de http://www.infoleg.gob.ar.

- Poder Ejecutivo Nacional. (2018). Decreto 683/18. *Reglamentacion de la Ley de Defensa de las Fuerzas Armadas.* Recuperado de http://www.infoleg.gob.ar.

- Poder Ejecutivo Nacional. (2017). Decreto 577/2017. *Creación del Comité de Ciberseguridad*. Recuperado de http://www.infoleg.gob.ar.

- Presidencia de la Republica de Lituania. (2014). *Ley de Ciberseguridad.* Vilnius: Presidencia de la Republica de Lituania.

- Richards, J. (31 de agosto de 2016). *International Affairs Review*. Recogido de http://www.iar-gwu.org/node/65

- Sepetich, S. (2016). Ciberoperaciones aplicadas al Teatro de Operaciones. ESGC, Buenos Aires.

- Trama, G. (2017). *Operaciones cibernéticas: su naturaleza, propósito y ejecución.* Buenos Aires: Escuela Superior de Guerra Conjunta de las Fuerzas Armadas.

- Thomas. T. (2017). " *El carácter evolutivo de como Rusia hace la Guerra*";Military Review

- Williams Brett T, The Joint Force Commander's Guide to Cyberspace Operations, Joint Force Quarterly 73, 2nd Quarter 2014, P. 14; Disponible en: http://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-73/jfq-73_12-19_Williams.pdf